A RESPONSIBILITY FRAMEWORK FOR INFORMATION SECURITY

Shaun Posthumus[1] and Rossouw von Solms[2]
[1]Nelson Mandela Metropolitan University, Shaun.Posthumus@nmmu.ac.za; [2]Nelson Mandela Metropolitan University, Rossouw.VonSolms@nmmu.ac.za

Abstract: This paper demonstrates that information security is more than a technical issue, through the development of an information security responsibility framework that shows consideration for strategic and legal issues as well. It is important that information security be viewed as both a governance challenge and a management responsibility. In order to achieve this this paper addresses information security governance and the board's participation in directing and controlling security efforts. Furthermore information security management is addressed in order to demonstrate how information security should be implemented. Once a comprehensive picture of the information security function has been established, the roles of various individuals in terms of information security are discussed and mapped out in the responsibility framework in order to demonstrate the true scope of an organizations information security function.

Key words: Corporate Governance; Information Security Governance; Information Security Management; Responsibility; Accountability

1. INTRODUCTION

The storage, processing and transmission of business information has been greatly facilitated by the development of computers and computer networks and the widespread implementation of such information technology (IT) resources. These developments have enabled organizations to perform business transactions with their customers, suppliers and other business partners with greater efficiency and speed. However, Entrust (2004,

p. 3) states that "the very openness and accessibility that stimulated the adoption and growth of private networks and the Internet also threaten the privacy of individuals, the confidentiality of information and the accountability and integrity of transactions." For this reason information security, is a business priority and should be integrated into an organization's business processes, with responsibilities assigned to all concerned individuals (BS 7799, 1999). This involves more than merely addressing technical issues, at the department level that may generate information security risks, as information security is also a strategic and possibly a legal concern (Birman, 2000). Several sources, including Entrust (2004), Swindle and Conner (2004) and Posthumus and von Solms (2004) have asserted that information security efforts should include executive management and board-level participation through sound information security governance endeavors. These efforts should then be supported by a well planned information security management strategy that exemplifies the board's and executive management's guidance in terms of information security direction. In order for an organization to make a success out of its information security program, everyone in an organization should know their responsibilities in terms of information security.

It is the objective of this paper to highlight the information security responsibilities of various individuals within an organization, from both a governance and management perspective, through the development of an information security responsibility framework. Such a framework serves to draw attention to the fact that information security is in fact both a governance challenge and well as a management responsibility that involves more than merely an organization's operational or technical managers (IT Governance Institute, 2005). In order to successfully motivate the responsibility framework, this paper firstly discusses the importance of corporate governance and then information security governance, as an important responsibility of the board. Information security management is then discussed with the intention of demonstrating the significant role management plays in implementing information security based on the board's direction and guidance in this regard. Once a more comprehensive picture of the entire information security function has been established in this way, various information security roles and responsibilities are addressed. These roles and responsibilities are then mapped out to form the responsibility framework, highlighting where key personnel fit in, and thus demonstrate the true scope of the information security function.

2. CORPORATE GOVERNANCE

Corporate governance is the system that dictates how an organization is directed and controlled. It is most certainly a very important function in any organization. In order to clearly express the importance of corporate governance, it should be analyzed more closely.

2.1 What is Corporate Governance?

Sir Adrian Cadbury, in the foreword of Corporate Governance: A Framework for Implementation, asserted that "corporate governance is concerned with holding the balance between economic and social goals and between individual and communal goals ... the aim is to align as nearly as possible the interests of individuals, corporations and society." (World Bank Group, 1999). This definition clearly suggests that there are a wide variety of issues that organizations need to consider in order to operate effectively in such a dynamic business environment as that which is found to be the case today.

Corporate Governance is ultimately all about sound leadership efforts (King Report, 2001). Sound leadership and good corporate governance are exemplified by the expression of several essential characteristics. These characteristics include accountability, responsibility, discipline, transparency, independence, fairness and social responsibility (King Report, 2001). An organization's board of directors must practice fairness, transparency, accountability and responsibility in every action taken, as well as remain accountable to their organization but nonetheless act responsively and responsibly where the stakeholders are concerned (King Report, 2001).

Good corporate governance is an important function in an organization, but there is a need to further clarify this statement by exploring why.

2.2 Why is Corporate Governance Important?

The most reasonable motivation for why corporate governance is so important in all organizations today is that these organizations have to realize that they should not attempt to function autonomously from the social orders or environments in which they exist (King Report, 2001). This is because, according to Thompson and von Solms (2003), organizations are a more direct presence to the general public than government. Therefore organizations should be compelled to demonstrate those characteristics that constitute good governance endeavors if they hope to gain the trust and support of the community or markets that they service. If these organizations fail to demonstrate characteristics such as transparency, responsibility or

accountability, for example, its executive leadership may be deemed untrustworthy, thus resulting in the financial demise of these organizations and therefore negatively effect the country's economy in some way (King Report, 2001).

Ultimately the quality of an organization's governance practices is really the only means of assurance its shareholders have that they will receive good returns on their investments in an organization (King Report, 2001). Corporate governance is therefore important because it is the mechanism that ensures that the best interests of an organization's shareholders are catered for. More specifically, corporate governance accomplishes this by regulating the use of an organization's resources in an appropriate manner, and placing accountability and responsibility onto those that govern the use of those resources (World Bank Group, 1999).

Good corporate governance can therefore be seen as the key to economic success and the stability of an organization. However, if corporate governance is not effectively implemented, some very negative consequences may transpire.

2.3 The Implications of Poor Corporate Governance

The poor corporate governance practices of the past have resulted in greater external scrutiny over the way companies operate today. As a result of such ineffective governance practices, boards of directors everywhere are now required to comply with a myriad of new laws and regulatory compliance mandates. The consequences of noncompliance with these stipulations involve swift legal action in the form of strict financial penalties or lengthy prison terms (Trillium Software, 2004). Thus regulatory intervention is obviously not the outcome of desire. Such intervention usually results in a tarnished corporate reputation and furthermore affects consumer and investor trust (Vericept Corporation, 2004).

Various legislative requirements aim to remind executives and boards of their corporate accountability and responsibility. However, there is a need to promote self governance, through an improved system of corporate governance, as an alternative to more legislation (Entrust, 2004). For this reason executive management and the board must ensure that they remain in complete control over their organization by understanding the full scope of their duties. This will ensure that their organization's valuable resources are not exploited in any way and the shareholders interests are preserved.

Since information is such an important asset to an organization it is the board's duty to ensure that this resource is also appropriately governed, the same as any resource. The Corporate Governance Task Force (2004), in the preface of Information Security Governance: A Call to Action, states that

"the road to information security goes through corporate governance". Therefore the board needs to understand their role with regard to protecting information. Hence information security governance is a very important aspect of corporate governance.

3. INFORMATION SECURITY GOVERNANCE

Information security has become a business priority that demands the attention of corporate board's and executive management. Therefore there is a need to explore information security governance in order to demonstrate the role of the board in terms of protecting vital business information assets.

3.1 What is Information Security Governance?

The Corporate Governance Task Force (2004, p. 5) states that "corporate governance consists of the set of policies and internal controls, by which organizations, irrespective of size or form, are directed and managed. Information security governance is a subset of organizations' overall governance program." Therefore information security governance would include board-level involvement in terms of directing and controlling an organization's information security efforts through effective policies, beginning with the creation of the corporate information security policy, and internal controls that govern the use of their business information assets.

Business information is very important to an organization, because having the right information at the right time is essentially what gives an organization a competitive advantage over others (Gerber & von Solms, 2001). For this reason the board must ensure that the confidentiality, integrity and availability of business information are maintained, in order to protect the interests of the shareholders and generate business value. Information security governance, aims to achieve this by focusing on risk management efforts, reporting and accountability with regard to the use of business information assets (Corporate Governance Task Force, 2004). Moreover, the corporate information security policy is the means by which the importance of these activities is communicated to the organization by the board through the expression of information security goals and objectives for confidentiality, integrity and availability. This ensures that the risks affecting these characteristics of information are all adequately minimized to an acceptable level.

Information security governance is thus essential because it ensures that there is board-level involvement in terms of directing and controlling an

organization's information security program, however there is a need to further clarify why this governance function is so important.

3.2 Why is Information Security Governance Important?

The vast implementation of computers and computer networks, which serve as a tool for service enablement and business value creation, also have the potential to significantly threaten the confidentiality, integrity and availability of business information. Due to the ease of accessibility to information and business services through the Internet and other networks, information is now primarily exposed to three fundamental elements that create potential risks. These three elements include firstly, the technology, which is used to store, process and transmit information; secondly, the people, i.e. customers and staff who access this information through various private networks and the Internet and thirdly, the business processes that deliver a particular business service that an organization provides (BS 7799, 1999). Information security governance is important because it brings accountability to each of these three elements, which are key components of corporate governance (Swindle & Conner, 2004). Promoting such accountability and responsibility for each of these elements of corporate governance is extremely important because of the many legal and regulatory pressures that boards of directors face today.

Once the board has understood the importance of information security governance as part of their corporate responsibilities and as a way to preserve the interests of their shareholders more fully, it would be necessary to explain how this function can be implemented further.

3.3 How can Information Security Governance be Implemented?

Information security can be said to be a priority of the board, and thus effective information security governance efforts are essential. Such efforts must enable the board to determine exactly what information security objectives their organization should fulfill in order to precisely define their information security direction and communicate such direction to the rest of the organization via the corporate information security policy. This would therefore serve to support the implementation of an accurate system of internal control. In order to ensure that the corporate information security policy communicates accurate information security objectives to the organization the board has to become aware of both internal and external

security requirements and guidelines (Posthumus & von Solms, 2004). In other words they need to identify the security requirements that various sources outside of their organization have recommended, as well as identify internal security requirements based on the specific needs of their organization. These security requirements specifically include: firstly, the requirements to protect the IT infrastructure; secondly, the business requirements that preserve the confidentiality, integrity and availability of information; and thirdly, any legal, regulatory or statutory requirements (Humphreys, Moses, & Plate, 1998). These requirements together with the guidance of industry best practices and well-regarded security standards, like BS 7799 (1999), help the board to establish the foundation for an effective approach to information security (Posthumus & von Solms, 2004), beginning with the accurate definition of information security goals and objectives. Such an approach will most assuredly bring accountability to people, process and technology elements through a well planned information security policy that promotes effective risk management and reporting mechanisms.

Previous research conducted by Posthumus and von Solms (2004), entitled "A Framework for the Governance of Information Security", which has been published in Computers and Security, motivated the development of a framework for information security governance and the communication of an effective information security policy. Figure 1 illustrates this framework, as it was developed and discussed in the paper. The framework draws attention to several major security requirements and how they all contribute in order to guide the board in terms of accurate information security decision making and the development and communication of the corporate information security policy.

Once the board has expressed their support of information security through sound governance efforts, management must then implement information security in the organization through an effective information security management strategy.

4. INFORMATION SECURITY MANAGEMENT

Information security management is an important step toward fulfilling the stipulations of the board in terms of information security, based on various identified internal and external security requirements. Hence information security management should be explored in more detail.

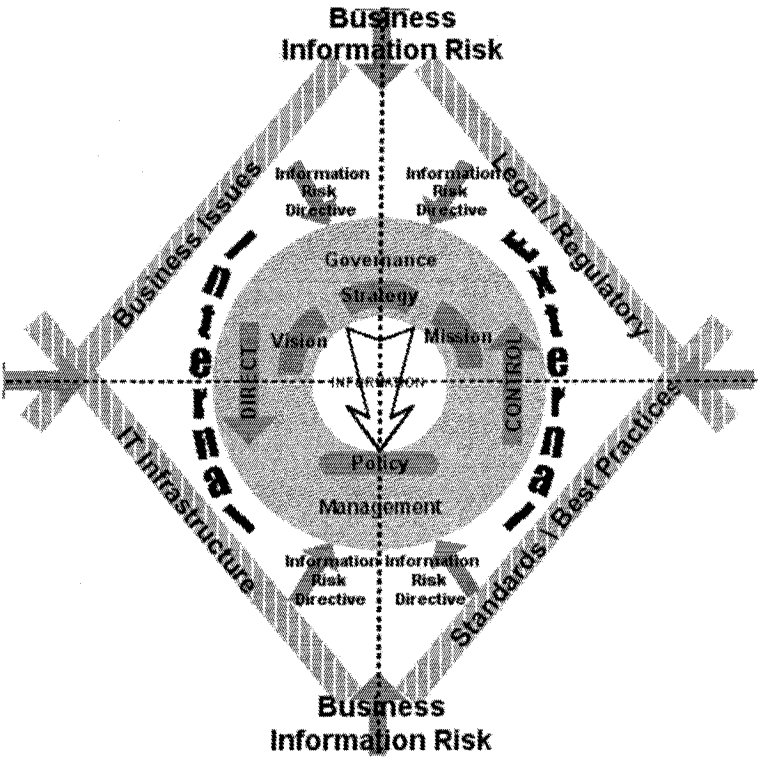

Figure 1. An Information Security Governance Framework

4.1 What Is Information Security Management?

Information security management is the process of carrying out various activities that facilitate the preservation of an organization's business information assets. This process is an expression of the information security objectives, which were stipulated by the board. Basically, information security management involves implementing security measures that exemplify the instructions of an organization's security policy, various security procedures and other security programs (Whitman & Mattord, 2003). Information security management aims to influence organizational culture (Whitman & Mattord, 2003), in order to create a secure information environment and mitigate business information risk.

Information security management is a continuous process, requiring constant review and adjustment in order to keep up with the latest technology developments and their associated risks (Whitman & Mattord, 2003) and to further ensure that the organizations information security goals

and objectives remain fulfilled to the fullest extent. There are essentially six consecutive phases that constitute a successful information security management program. These phases include investigation, analysis, logical design, physical design, implementation and maintenance and change (Whitman & Mattord, 2003). The primary intention of an information security management program is to identify particular threats and create particular security controls that counteract those threats (Whitman & Mattord, 2003) and hence preserve confidentiality, integrity and availability of business information.

It is essential to differentiate between information security management and information security governance, in order to highlight why each of these functions are so important in terms of securing business information assets.

4.2 The Difference between Information Security Management and Information Security Governance

Information security governance and information security management together form the unified process that constitutes an organization's broader information security function. Each of these activities has a particular contribution to make in terms of information security and are thus both essential.

According to the King Report (2001) it is the responsibility of the board to effectively direct and control all aspects of their organization through sound governance efforts. This therefore includes directing and controlling information security efforts as this must become a part of an organization's key business operations (Entrust, 2004). Information security governance is thus a board-level responsibility and expresses the board's commitment to information security with the development of a corporate information security policy, also called a security program policy that outlines the organization's vision, mission and information security direction (Whitman & Mattord, 2003). The board further controls security efforts through reporting mechanisms. Frequent reports enable the board to review the effectiveness of their guidance with regard to information security and redirect such efforts as necessary. In addition to this various board-level committees make recommendations to the board so that they can make accurate decisions and effectively govern information security. Thus information security governance is all about strategy setting and the communication of information security objectives.

Information security management, on the other hand, is more concerned with how the stipulations of the board, expressed in the corporate information security policy, are implemented within an organization. Therefore activities such as identifying specific security controls and

formulating procedures to counteract risks form the basis of the information security management function. Literature suggests that information security management usually does not include personnel beyond the ranks of an organization's chief information officer (CIO). Usually the chief information security officer (CISO), who is not in an executive level position, is responsible for managing an organization's information security program (Whitman & Mattord, 2003). Information security management is thus a management responsibility and does not include board-level participation. It is more concerned with how security will be implemented in the organization.

In order to gain a clearer understanding of what information security management actually entails, a more detailed discussion regarding this function is on order.

4.3 Information Security Management: The Process

Information security management begins with clear direction. This is achieved with the guidance of accepted security standards and codes of practice such as BS 7799 (1999). Additionally, the issuing of a corporate information security policy helps to express the commitment of the organization toward protecting the confidentiality, integrity and availability of business information. Hereafter a series of activities that aim to realize this commitment commence. Some of these activities include an initial assessment of various potential risks to information which is then followed by some form of risk management strategy. This enables an organization to identify and implement an assortment of physical, technical and operational security controls. Examples include burglar alarms, access control mechanisms and more specific security policies, procedures, standards and guidelines respectively. Some other activities that are carried out through an information security management program include staff training in security practices, testing the security infrastructure, detecting and responding to various security incidents and business continuity planning (Entrust, 2004). In addition to these activities auditing the security function and reporting to the board on its effectiveness are key elements that promote accountability and responsibility for the broader information security function.

However, in order to effectively enforce accountability and responsibility for information security throughout an organization, various individuals need to fully understand the roles they play in this regard.

5. INFORMATION SECURITY TASKS, ROLES AND RESPONSIBILITIES

Information security is a process that requires a commitment from many key individuals in an organization to ensure its effectiveness. Therefore there is a need to identify the key role players and examine their responsibilities more closely.

5.1 The Role of the Board of Directors

By this stage it should be clear that the primary role of the board is to oversee the interests of the shareholders by effectively directing and controlling an organization and ensuring that all resources are appropriately utilized. Therefore with regard to information as a business resource the board must understand its significance as well as the significance of protecting it through successful information security efforts (Corporate Governance Task Force, 2004). Additionally the board must support the establishment and implementation of a robust information security program by setting the information security direction and communicating this through the corporate information security policy. The board must also receive management reports on the utility and effectiveness of their security program (Corporate Governance Task Force, 2004). This enables the board to ensure that their organization's security efforts remain on track.

5.2 The Role of Board Committees

Board committees facilitate the board in carrying out their duties efficiently and show that the board's responsibilities are being appropriately accomplished (King Report, 2001). There are several board committees that can assist the board with their responsibility for information security. These committees specifically include: firstly, the IT oversight committee; secondly, the audit committee and lastly, the risk management committee. The role of the IT oversight committee is to advise the board on an appropriate IT strategy for an organization (IT Governance Institute, 2004). Thus the IT oversight committee must ensure that an organization's IT strategy supports information security, since IT is so closely linked to this resource (IT Governance Institute, 2004). The audit committee is responsible for conducting performance reviews of an organization's system of internal control and must also review all legal and regulatory compliance efforts (King Report, 2001), including that of information security. Lastly, the risk management committee advises the board regarding corporate accountability

as well as management, reporting and assurance related risks (King Report, 2001). The risk management committee's terms of reference include technology risk, operational risk, disaster recovery risk, and compliance and control risks (King Report, 2001). Thus, generally speaking, the information provided to the board by these various board committees, regarding the effectiveness of current security efforts further facilitates the board in the review of the organization's security policy.

5.3 The Role of the CEO

The chief executive officer (CEO) is responsible for overseeing the entire information security program of the organization (Corporate Governance Task Force, 2004), and sign off the information security policy. Additionally he must oversee compliance efforts and enforce accountability for such efforts (Corporate Governance Task Force, 2004). Furthermore the CEO must also report compliance issues to the board, highlighting the level of acceptable risk, weaknesses in current information security practices and plans to strengthen these practices (Corporate Governance Task Force, 2004). The CEO must also allocate responsibility, accountability and authority for various security functions to the right personnel in an organization and appoint someone as the senior information security officer (Corporate Governance Task Force, 2004).

5.4 The Role of the CIO

An organization's CIO typically makes recommendations to the CEO on the strategic planning efforts affecting the administration of an organization's information resources (Whitman & Mattord, 2003). Furthermore the CIO converts an organization's strategic plans into strategic plans for information and information systems (Whitman & Mattord, 2003). Additionally, the CIO collaborates with other non executive managers in order to develop plans of a tactical and operational nature for the management of information and information systems. Such efforts would entail setting the policies and procedures for information security (Corporate Governance Task Force, 2004). Thus the CIO plays a major role in the drafting of the organization's information security policies.

5.5 The Role of the CISO

The CISO is responsible for the overall information security management function (Whitman & Mattord, 2003). Some of his responsibilities in terms

of this include, collaborating with the CIO on strategic information security plans, establishing tactical plans and collaborating with other security managers on operational security plans (Whitman & Mattord, 2003). Additionally the CISO must plan the information security budget i.e. assign resources for executing information security and act as the representative for all other security personnel (Whitman & Mattord, 2003). The CISO thus plays a major role in implementing the specifications of the organization's information security policy at a management level.

5.6 The Role of Data Owners (The Business Unit Leaders)

One of the typical responsibilities of the business unit leaders includes implementing the specifications of more specific security policies and procedures (Corporate Governance Task Force, 2004). It is also their responsibility to audit and review the effectiveness of various security procedures as well as communicate the security policies and procedures to other subordinate personnel through various staff training initiatives (Corporate Governance Task Force, 2004). Additionally they must enforce compliance with the security policies (Corporate Governance Task Force, 2004).

These various security roles and responsibilities span the entire organization, involving personnel in both management and governance positions, including the board of directors. This helps to demonstrate that information security is in fact more than a technical issue, as Entrust (2004), the Corporate Governance Task Force (2004) and Posthumus and von Solms (2004) have motivated. Therefore in order to clearly elucidate how information security should be addressed as more than a technical issue, to include consideration for the legal and business issues as well, it should be shown how key individuals collaborate. This is best achieved through an information security responsibility framework.

6. AN INFORMATION SECURITY RESPONSIBILITY FRAMEWORK

An information security responsibility framework helps to demonstrate the true scope of the information security function in an organization as it involves both governance and management support in order to address the full spectrum of information risks and security requirements.

6.1 The Governance Side

The governance side of the framework involves actions by executive management and the board in order to address the strategic issues of information security from a business and legal perspective. In this regard, the CIO should consult with the IT oversight committee on the alignment of business and IT, which is part of this committee's duties (IT Governance Institute, 2004), and should also address information security, as this should be regarded as a business issue. The CIO should also consult with the audit committee regarding internal control and compliance efforts. Furthermore, the CIO advises the CEO on strategic plans regarding information management (Whitman & Mattord, 2003), and the information security efforts that are in place to preserve information. The CEO then reports all issues regarding the information security function to the board (Corporate Governance Task Force, 2004), along with the status of legal compliance efforts. The board must then direct and control the security function guided by the advice of the IT oversight committee and the audit committee to align the corporate information security policy with current business strategies and objectives.

6.2 The Management Side

The management side if information security involves actions by non executive management and the CIO in order to address the implementation issues of information security from an infrastructure and best practice point of view. It is important to note that the CIO plays a major role in the entire information security function, as this individual has contributions to make in terms of both the governance and the management of information security. In the context of information security management, the CIO works closely with the CISO to develop strategies for information security (Whitman & Mattord, 2003), that would involve activities such as risk management, risk monitoring, reporting and so forth. These strategies consider reports from the CISO concerning all issues regarding the status of the current information security management function. The status of the organization's information security management function is made clear to the CISO by reports from the business unit leaders concerning the effectiveness of the security function in various departments. The business unit leaders, or department heads, are also responsible for ensuring that all employees are trained in security awareness and comply with information security policies, practices and procedures so that they act responsibly with regard to the organization's information assets (Corporate Governance Task Force, 2004).

Figure 2 illustrates the responsibility framework for information security which involves the commitment of both the management and governance components in an organization in order to fulfill all of the necessary security requirements and effectively secure business information assets. An important point to note with respect to the framework is that it can be closely linked to the information security policy. More specifically, the corporate information security policy covers much similar ground to the framework. A key feature of the information security policy is the delegation of security responsibilities. Thus the framework can further facilitate the development of the information security policy as it can be viewed as a road map to better information security strategy development.

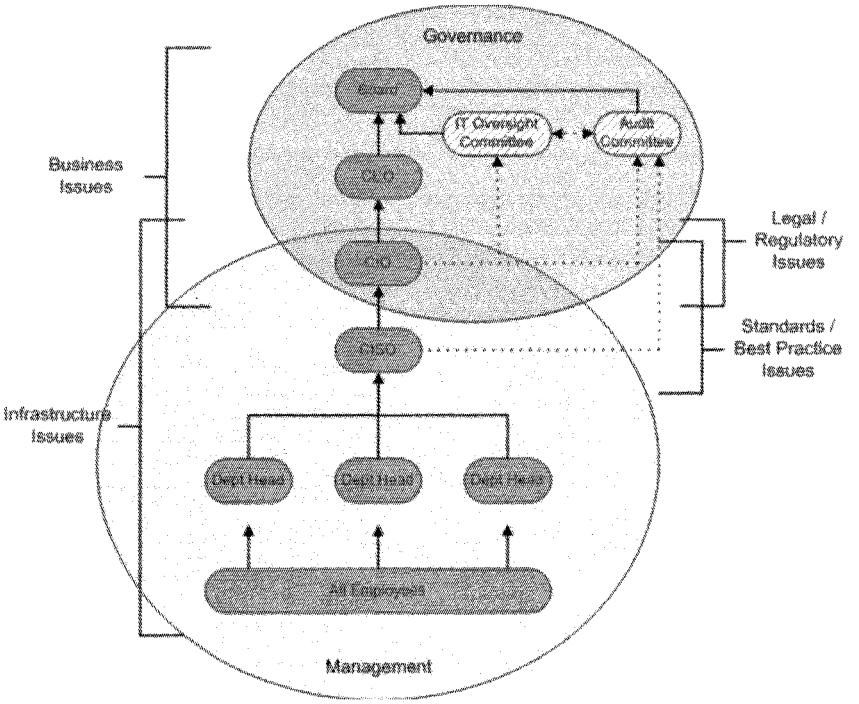

Figure 2. An Information Security Responsibility Framework

7. CONCLUSION

The development of an information security responsibility framework helps to show that both governance and management support are essential constituents of a comprehensive information security function. Both

governance and management support enables an organization to satisfy the full spectrum of information security risks by addressing all information security requirements. Thus such a framework helps to illustrate that the true scope of the overall information security function involves a lot more than merely addressing technical issues (Entrust, 2004) but also includes consideration for strategic and legal issues as well (Birman, 2000). Consequently this enables the board to have complete control over an organization's resources, including information and in this way better preserve the shareholders interests and effectively govern their organization.

REFERENCES

Birman, K. P., 2000, The next generation internet: Unsafe at any speed. *IEEE Computer, 33*(8), 54–60.

BS 7799, 1999, *BS 7799: Code of Practice for Information Security Management as a base for Certification.*

Corporate Governance Task Force, 2004, *Information Security Governance: A Call To Action.* Available from: `http://www.cyberpartnership.org/InfoSecGov4_04.pdf`.

Entrust, 2004, *Information Security Governance (ISG): An Essential Element of Corporate Governance.* Available from: `http://itresearch.forbes.com/detail/RES/1082396487_702.html`.

Gerber, M., & von Solms, R., 2001, From risk analysis to security requirements. *Computers and Security, 20*(7), 577–584.

Humphreys, E. J., Moses, R. H., & Plate, E. A., 1998, *Guide to BS7799 Risk Assessment and Management.* British Standards Institution.

IT Governance Institute, 2004, *IT Strategy Committee.* Available from: `http://www.ITgovernance.org/resources.htm`.

IT Governance Institute, 2005, *Information Security Governance: Guidance for Boards of Directors and Executive Management.* Available from: `http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=15998`.

King Report, 2001, *The King Report on Corporate Governance for South Africa.* Available from: `http://www.iodsa.co.za/IoD%20Draft%20King% 20Report.pdf`.

Posthumus, S., & von Solms, R., 2004, A framework for the governance of information security. *Computers and Security, 23(8)*, 638–646.

Swindle, O., & Conner, B., 2004, *The Link between Information Security and Corporate Governance.* Available from: `http://www.computerworld.com/securitytopics/security/story/0,10801,92915,00.html`.

Thompson, K., & von Solms, R., 2003, *Integrating information security into corporate culture.* Masters dissertation, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

Trillium Software, 2004, *Corporate Governance and Compliance: Could Data Quality Be Your Downfall?* Available from: `http://www.trilliumsoftware.com/success/dqic.pdf`.

Vericept Corporation, 2004, *Preventing Identity Theft and Loss of Intellectual Property: The Importance of Information Security in Internal Controls and Corporate governance.* Available from: http://www.vericept.com/Downloads/WhitePapers/Vericept_Fraud_IdentityTheft_WP.pdf.

Whitman, M. E., & Mattord, H. J., 2003, Principles of information security. In (pp. 153 – 190). Course Technology.

World Bank Group, 1999, *Corporate Governance: A Framework for Implementation.* Available from: http://www.worldbank.org/html/fpd/privatesector/cg/docs/gcgfbooklet.pdf.