CHAPTER FOUR:
ENTITIES RESPONSIBLE FOR INFORMATION SECURITY GOVERNANCE

4.1 Structure of chapter

This chapter aims at providing a point of departure for sound information security governance. Within this chapter the entities responsible for information security governance are identified and given initial guidance on how to effectively face the challenges of the information age.[1]

The objective of this chapter is to address the following two questions regarding the discipline information security governance, namely:

(i) Who should be concerned with information security governance? and

(ii) Why should these entities be concerned with this discipline?

Outline of chapter:

Part 2: offers insight into the question why information security needs to be governed;

Part 3: gives an overview of what the concept "board" entails, its traditional role within the organisation, as well as its position in the light of the information age. It will go further to discuss the concept of "management", again evaluating management's traditional role before focussing attention on how the information age has altered this role; and

Part 4: highlights some of the challenges facing the board and managers in the information age.

---

[1] Keep in mind that chapter two identified the board of directors and top management as the primary role-players in the information security discipline. The reader should however be mindful of the fact the discussion which follows is not intended to serve as a comprehensive discussion of the board and management's roles within the organisation. The aim of chapter 4 is only to provide a brief overview thereby providing a setting for the chief object of contemplation, information security governance.

It is concluded that the responsibility for information security governance resides in two entities, namely the board of directors and top management. The board is accountable to the owners of the company. The board will furthermore be held accountable for information security governance, regardless of their knowledge or lack thereof on the subject-matter.[2] Consequently within the board the ultimate responsibility for information security governance reside. Therefor they need to be involved in and committed to information security governance if they wish to escape liability.[3]

Top management is in turn answerable to the board on this subject-matter. Although these two entities function interdependent of one another, their nature, responsibilities, accountability and composition are inherently different. To understand the managerial challenges information security governance present to the board and top management the "traditional roles" these two entities played preceding the information age must first be explored. Only once their traditional roles are understood can one begin to assess the influence the information age has had on the organisation as a whole, as well as on the people responsible for the governance and management of the organisation. It must be acknowledged that the advances made in the information technology and information security arenas do not render the traditional roles of these two entities absolute, in reality the contrary proves to be true: the information age augments, enhances and cultivates the role these two entities play within the organisation.

4.2. Introduction

As have already been discussed in the preceding chapter, information security governance is a specie of the overall governance concept. The only difference is that information security governance functions in a different medium, namely cyberspace. Considering the fact that responsibility for all governance activities ultimately reside in

---

2 IT Governance Institute "Information security governance" (2001) http://wwwITgovernance.org 11.

3 Roberts *Computer Security* (1990) 118.

the board of directors and top management,[4] it should follow that the responsibility for information security governance will also reside in the board and top management. This responsibility can at present not be delegated.[5] However, in the past, because of the complexities associated with information security, the responsibility thereof was normally delegated to a specific department or unit.[6] Consequently the board did not incur liability if something did go wrong.[7] This approach to information security resulted in management becoming "detached from technology,"[8] having little or no knowledge of the subject matter,[9] and indirectly loosing control over one of its most important assets.[10] Another problem that materialised as a result of this approach was that information security was solely addressed as a technical issue, business considerations and requirements were not brought into the equation. Information security was seen in isolation of the rest of the business operations. At present organisations are beginning to realise that information security is not a technology issue, but a business issue.

4.3 Entities concerned with information security governance

Two entities that should pay considerable attention to the issue of information security governance are the board and top management, as they may incur personal liability for non-compliance/non-adherence to this discipline.[11] A clear distinction should however be drawn between these two entities. Although there exist an interrelationship between management and the board that is based on trust, their accountability, responsibilities and functions are inherently different.[12] Furthermore the concepts of management and governance should not be used interchangeably as they involve two very different activities. Governance may be seen as "existing outside the phenomenon of management

---

4 (n 3) 13.
5 Warman *Computer Security within Organizations* (1993) 75.
6 (n 5) 79.
7 (n 2) 11.
8 (n 5) 79.
9 They might have required reports to be delivered on a periodical basis, just to keep themselves in a comfort zone.
10 (n 5) 79.
11 Carver and Oliver *Corporate Boards that Create Value* (2002) xii.
12 (n 11) 51.

and inside the phenomenon of ownership," and will be the responsibility of the board, whereas the management of the organisation will be vested in managers.[13] Because of these inherent differences it is necessary to launch an investigation into the nature and composition of each of these two entities respectively.

4.3.1 The board

4.3.1.1 Board of directors defined

A board may be defined as "a body accountable to the owners that operates as the highest initial authority in a company, and therefor the value it creates is translating owners' wishes into company performance."[14]

4.3.1.2 Composition of the board

The board should be composed of a balance of executive and non-executive directors, preferably with a majority of non-executive directors.[15] Independent directors play a pivotal role, as is evident from the fact that all committees must be chaired by an independent director. [16]

There is a new[17] trend amongst global organisations to appoint an IT director as a member of the board.[18] This appointment is usually driven by fear. Fear of new technology, fear of their own ignorance and fear of competition.[19] The elevation of IT-related matters to board-level were driven by the realisation that IT has a dual function as

---

13 (n 11) xxi.
14 (n 11) 8.
15 Wixley and Everingham *Corporate Governance* (2003) 16.
16 (n 15) 18-19.
17 The term "new" is relative, as this practice has been ongoing since 1985. It is however just recently that it has taken off.
18 Grindley *Managing IT at Board Level* (1995) 14.
19 (n 18) 15.

a business supporter and enabler. Consequently, if this component of the business is neglected, it may reflect negatively on the bottom-line.[20]

Additional reasons that may be advanced for appointing an IT director are:

(i) IT directors will aid in giving insight into the cost associated with IT;[21] and

(ii) It is useful to have a knowledgeable person on the board to whom IT related questions may be referred. This gives fellow-members a sense of security.[22]

4.3.1.3 Authority vested in the board

A few general principles should be kept in mind when discussing the authority vested in the board.

(i) The main function of the board is to govern the organisation on behalf of its owners.[23] "Board must act as a link between owners and management, directing and controlling the company on the owners' behalf."[24] Therefor the board may be seen as the intermediary between owners and managers.[25] Furthermore within the hierarchy of the organisation the highest authority is vested in

---

20 (n 18) 65.
21 (n 18) 70.
22 ibid.
23 (n 11) 8.
24 (n 11) 5.
25 (n 11) 28.

the board, under that of the owners.[26] The source of the board's authority is therefor the owners of the company. [27]

(ii) The board is an organ of the organisation. "When an organ of the company acts it is for all practical purposes the company itself which acts."[28] Only certain entities qualify as being organs of an organisation. Within the organisational structure this term is reserved for the board of directors, general meeting of members, and in anomalous circumstances the managing director.[29]

(iii) "The board is accountable for everything about the company."[30] Because of the fact that the board is the highest organ of authority it inevitably carries with it the responsibility of accountability.[31] The board will therefor be held responsible for the performance of the organisation, as well as for any and all projects undertaken and decisions made by the organisation.[32] Although the board is encouraged to utilise its delegation powers it is unable to delegate and/or abdicate its inherent responsibility to the organisation.[33]

(iv) The board is accountable to stakeholders and not just shareholders.[34]

---

26 (n 11) 6.

27 The question may be asked who are the owners of the organisation? There is no clear answer to this question. At present various debates are raging on this issue. Some maintain that the term "owners" are limited to shareholders, others argue that employees of the organisation must also be included, then there are those who assert that a broad definition for owners must be adopted that will include all stakeholders. Finegold, Lawler and Conger "To whom are boards accountable?" *The Corporate Board* (2001) 17-22.

28 Cilliers, Benade, Henning, Du Plessis, Delport, De Koker and Pretorius *Corporate Law* (2000) 84.

29 ibid.

30 (n 11) 8.

31 (n 11) 7.

32 ibid.

33 ibid.

34 Cohen and Boyd *Corporate Governance and Globalization* (2000) 163.

(v) "All authority and accountability is vested in the board as a group."[35] Consequently, the board can only act, make decisions and exercise authority as a group.[36] Individual directors will be unable to make unilateral decisions or take unilateral actions without the consent of their fellow board members.[37]

4.1.3.4 Principal board activities

Boards are responsible for the management of the company. Assimilated into this are legal, ethical and social responsibilities. The board must have regard to their responsibilities to customers, employees, suppliers and stakeholders in general.[38] The following principal board activities may be identified:

(i) Give strategic direction and advice

All business operations evolve around a strategy. It is not expected of the board to develop the business strategy, it is however expected of the board to act as a consultant to the chief executive officer with regards to any questions, advice or recommendations he may need or require.[39] They are therefor acting in an advisory capacity sharing their skills, knowledge and expertise with management.[40] It is suggested by Conger [41] that because of the fact that "directors are not involved in the day-to-day development of

35 (n 11) 8.
36 (n 11) 28.
37 The authority to perform a specific action, transaction or decision may however be delegated to a single director. It is furthermore allowed for one member to try and influence his/her fellow-members in order to persuade them to agree with him/her on a specific topic. Apart from this they do not possess over the authority to act unilaterally. It furthermore stands to reason that management must act on instructions received from the board as a group. No member of management has to follow the instructions of a single director acting or making unilateral decisions Carver (n 11) 7; 29.
38 (n 11) 62.
39 Conger, Lawler and Finegold *Corporate Boards* (2001) 9.
40 (n 11) 3.
41 (n 39) 10.

strategy, they are often in a position to provide an objective and detached critique of its potential effectiveness."

(ii) Oversee strategy implementation and performance

The development of a strategy is only the first step in the strategy process. Even the best strategy will be rendered useless if it is not executed properly.[42] It is therefor suggested that boards must be involved throughout the strategy implementation process giving guidance, evaluating and monitoring performance.[43] The monitoring function may be performed by setting benchmarks and collecting independent information.[44]

(iii) Safeguards

The board acts as a "watchdog" for investors by monitoring, overseeing and evaluating actions of management and the overall performance of the organisation.[45] As a direct consequence of this management is answerable to the board in relation to its activities.[46]

---

42 (n 39) 11.

43 ibid.

44 (n 39) 12.

45 In order to provide the stakeholders of the organisation with some reassurance that their investment in the organisation is worth-while it is suggested that the board take the following steps:

(a) Performance evaluations may be used as a mechanism to achieve greater accountability while simultaneously increasing the effectiveness of the board. These evaluations should take place in fixed intervals and should evaluate not only decisions and actions of the board in its entirety but also that of individual board members. It is furthermore recommended that independent, objective third parties should conduct these evaluations;

(b) Periodic reviews of corporate governance practices within the organisation must be performed;

(c) Review the findings of (b) and benchmark it against industry standards; and

(d) Demand that directors render their resignation if they change their primary job or accept appointment to sit on the board of another company. Conger, Lawler and Finegold (n 39) 103; 177.

46 ibid.

(iv) Developing and evaluating the CEO

It is contended by Conger [47] that this involves one of the most important activities a board may perform. The reason being that (i) only the board has the authority to evaluate the CEO, and (ii) only the board has access to information on which this evaluation will be based.[48] The board is furthermore the only organ within the organisation that possesses over the necessary authority to select and remove the CEO where necessary. The board's evaluation function also extends to the evaluation of management.[49]

(v) Preventing and managing crisis

It is expected of boards to anticipate or develop "worst case scenarios" and identify corrective actions to be taken or measures to be implemented if these hypothetical situations ever materialise.[50] Boards must furthermore become more flexible, be able to meet on short notice and make decisions within a short time frame.[51]

(vi) Acquiring and allocating resources

Organisations need to have access to its resources, in order to take full advantage of business opportunities.[52] Resources over which an organisation may possess include but are not limited to,

47 ibid.
48 (n 39) 13.
49 Knepper and Bailey *Liabilty of Corporate Officers and Directors* (1998) 1.
50 (n 39) 15.
51 (n 39) 16.
52 ibid.

financial capital, human capital, business relationships and technology.[53]

(vii) It is the board's responsibility to ensure that senior management, as well as the organisation as a whole stay within the **boundaries of the law**. The board must gain assurance that these two entities are conducting themselves in an ethical manner.[54] In order to discharge these responsibilities effectively the board needs access to reliable information on how these entities behave.[55]

4.1.3.5 Characteristics of an effective board

Conger [56] suggest that boards must possess over the following four attributes in order to manage the organisation effectively and to perform the aforementioned activities efficiently:

(i) Information;
(ii) Knowledge,
(iii) Power; and
(iv) Rewards that motivates performance.

---

53 ibid.
54 (n 39) 14.
55 ibid.
56 (n 39) 21.

(i) Information

Information refers to "data about occurrence, events and activities that affect the business."[57] The traditional and contemporary business environment demand that boards have access to reliable information on:

(a) The performance of the organisation; [58]

(b) Operation and management of the organisation; [59]

(c) Business environment in which the operation functions; and [60]

(d) Competitors and how the organisation compare to them.[61]

With the advent of the information age and the Internet directors are exposed to a wealth of information. This unlimited supply of information does however represent a two-edged sword.[62] Directors are finding themselves in the fortunate position of having access to company information twenty-four hours a day, seven days a week, yet there is a very real danger that they will experience an **information overload**.[63] "With too little information, there is a risk that directors will be unable to accomplish their major objectives; too much information often is the equivalent of no information."[64] The problem of information overload therefor centers around the amount/quantity of information that the board requires, yet, the effectiveness and correctness of decisions taken by boards will depend to a large extend on the information available to them.[65]

In order to understand how the information overload occurs it must first be understood what type of information the board will be presented with. The information provided to the board may be subdivided into two main categories namely information on lead and lag indicators.[66] **Lag indicators** normally reflect the organisation's past accounting and

---

57 ibid.
58 ibid.
59 ibid.
60 ibid.
61 ibid.
62 (n 39) 133.
63 ibid.
64 (n 39) 82.
65 (n 39) 73.
66 (n 39) 75.

financial performance.[67] It focuses on the past and not on the present or future.[68] The reason why these indicators are so important is because these results are disclosed to the public and investors base their future decisions on them.[69] The board however needs to be provided with information on **lead indicators** (future performance), in order to make informed decisions on the direction in which the organisation is heading.[70]

To counteract this problem it is suggested that "information filtering" should take place.[71] The filters that must be in place will depend on external and internal factors influencing the organisation.[72] The information the board receives must furthermore relate to the directors specific area(s) of responsibility.[73] Therefor only information that is crucial to boardroom meetings and decisions must be furnished.[74] The problem of information overload may be limited to a great extend, if managers could be trusted to provide the board with only the relevant information they required. Ideally management must sort through the information and determine which information the board needs to be made aware off.[75] Keep in mind: "boards exist to govern, not become immersed in company operations, so information must facilitate corporate governance, not micromanagement."[76]

(ii) Knowledge

Knowledge refers to "the expertise and understanding that is resonant in a group or individual."[77] The board needs to possess knowledge in the following key areas:[78]

(a) Business strategy;

---

67 ibid.
68 ibid.
69 ibid.
70 ibid.
71 O'Brien *Management Information Systems* (1996) 455.
72 ibid.
73 (n 39) 76.
74 (n 39) 73.
75 (n 39) 82.
76 (n 39) 73.
77 (n 39) 21.
78 (n 39) 40-41.

(b) Leadership;

(c) Organisational issues;

(d) Relationships;

(e) Functional knowledge; and

(f) Ethics and the law.

(g) An additional key area that has emerged in recent years is knowledge of the **technology used within the organisation**. [79]

The knowledge requirements have changed significantly with the advent of the information age.[80] Several years ago it would not have been required of any member of the board to have any knowledge of, or even give regard to information technology and the Internet.[81] At present we find very few boards that do not regard the Internet as "a critical strategic concern."[82] As observed by Porter:[83]

> "Many have argued that the Internet renders strategy obsolete. In reality the opposite is true. Because the Internet tends to weaken industry profitability without providing proprietary operational advantages, it is more important than ever for companies to distinguish themselves through strategy. The winner will be those that view the Internet as a complement to, not a cannibal of, traditional ways of competing." [84]

"Knowledge that the board contain is largely determined by the members they select."[85] It is an unfortunate fact that many directors have vast knowledge and expertise of the bricks-and-mortar approach to organisations, as they were educated on the governance of

---

79 (n 39) 21.

80 (n 39) 49.

81 ibid.

82 ibid.

83 He observes that most dot.com as well as certain brick-and-mortar companies have ignored the rules of strategy completely when doing business on the Internet. "By creating separate Internet strategies instead of integrating the Internet into an overall strategy companies fail to capatalise on their traditional assets, reinforced me-too competition, and accelerate competitive convergence. Dot.com, first and foremost, must pursue their own distinctive strategies, rather than emulate one another or the positioning of established companies. They should break away from competing solely on price and instead focus on product selection, product design, services, image, and other areas in which they can differentiate themselves." Porter "Strategy and the Internet" (March 2001) *Harvard Business Review* 72;77;78.

84 Porter "Strategy and the Internet" (March 2001) *Harvard Business Review* 63.

85 (n 39) 132.

a company before information technology became the core of every organisation's existence.[86] A change in mindset is therefor required from governance of brick-and-mortar organisation to governance of a click-and-mortar. It is of the utmost importance that directors start making a conscious effort to become informed about the impact of, and consequences associated with, conducting business in the information age.[87] Directors should furthermore be encouraged to become more net-active, thereby familiarising themselves with the Internet and getting comfortable with conducting business and communicating on the Internet.[88] The board of directors as well as employees should be goaded to make use of the organisation's intranet when communicating. In the future we are bound to see videoconferences taking the place of traditional meetings, and directors will be kept informed via e-mail on the latest developments in the company.[89]

(iii) Power

"Power is the ability to make and influence decisions."[90] Within the context of this discussion the concept of power may be equated to that of authority, and authority can only be enforced if the board is respected and recognised as the highest authority within the organisation.[91] The board will only be respected if lower-level employees are

---

86 Applegate, McFarlan and McKenney *Corporate Information Systems Management* (1999) 3.

87 Various methods may be employed to educate them on this, for example by:
(a) Inviting external experts to speak on issues;
(b) Visiting to dot.com firms; and
(c) Senior management may be able to educate directors. Conger, Lawler and Finegold (n 39) 132.

88 (n 39) 132.

89 A move in this direction may already be observed in the JSE New Listing Requirements where schedule 23 expressly deals with the use of electronic media for the delivery of investor information. Issues dealt with under this schedule include: (i) electronic circulars and delivery; (ii) service providers; (iii) circulars on websites; (iv) evidence of electronic delivery; and (v) online proxy voting. Directors may furthermore obtain external viewpoints on how the outside world views the organisation by going on-line and conducting, for instance, automated searches of analyst reports, articles published in the press, specialised industry and technical publications Conger, Lawler and Finegold (n 39) 133;134;135.

90 (n 39) 21.

91 ibid.

convinced that the board is competent, objective and knowledgeable about the internal workings of the organisation.[92]

(iv) Incentives

"Rewards influence the willingness of individuals to commit their energy to perform a particular task."[93] All employees, regardless of their level of employment, expect to be rewarded for good performance, they will inevitably ask the question: "what is in it for me?"[94] Rewards may effectively be used as a "tool" to encourage and motivate directors to attend meetings, keep informed and to play a more active role within the organisation.[95] Rewards will generally be awarded based on a set of performance indicators relevant to a specific department or unit to whom the individual is assigned.[96]

Various **benefits** are offered by a rewards system:

(i) It fosters alignment within the organisation;[97]

(ii) Encourage employees to work harder and build commitment amongst them;[98]

(iii) Links what is expected of employees with what they achieve; [99] and

(iv) May serve as a retention mechanism, convincing valuable, skilled employees to stay with the organisation. [100]

---

92 ibid.
93 ibid.
94 Kaydos *Operational Performance Measurement* (1999) 149.
95 ibid.
96 It is contended by Wilson that rewards should not be viewed as "merely compensation or recognition programs. They are processes that translate strategic goals and values into action and define how people will be reinforced for their actions." Some examples of rewards include salary programs, incentives or bonus programs. Wilson *Rewards That Drive High Performance* (1999) 19.
97 Wilson *Rewards That Drive High Performance* (1999) 19.
98 ibid.
99 ibid.
100 ibid.

Ultimately a reward system that has effectively been implemented will result in "an environment where people are valued for achieving desired results"[101] thereby "improving their overall performance and gain a competitive advantage." [102] An organisation where a reward system is effectively implemented is characterised by achievement, excitement and fulfillment. [103]

(v) Opportunity and time

As a result of technology, information technology and the Internet we find an increase in speed with which everything takes place in the business environment. This makes the board's traditional approach to business inefficacious. The typical conduct of a board to meet four to eight times a year, set five-to-ten-year plans and set annual targets will prove to be highly ineffective because of the rapid rate at which everything is taking place and changes are occurring in the business environment. It should be made clear that it is unrealistic to expect of the board to be involved in the day-to-day running of the company. It is however expected of them to become more adaptable and flexible. As a result of this boards will have to accelerate the speed with which they make decisions, meet more frequently, and start using technology to their advantage by utilising this resource to keep informed, make decisions, and even conduct business meetings.

4.3.2 Management

The second entity that should be concerned with information security governance is top management.

---

101 (n 97) 293.
102 ibid.
103 (n 97) 4.

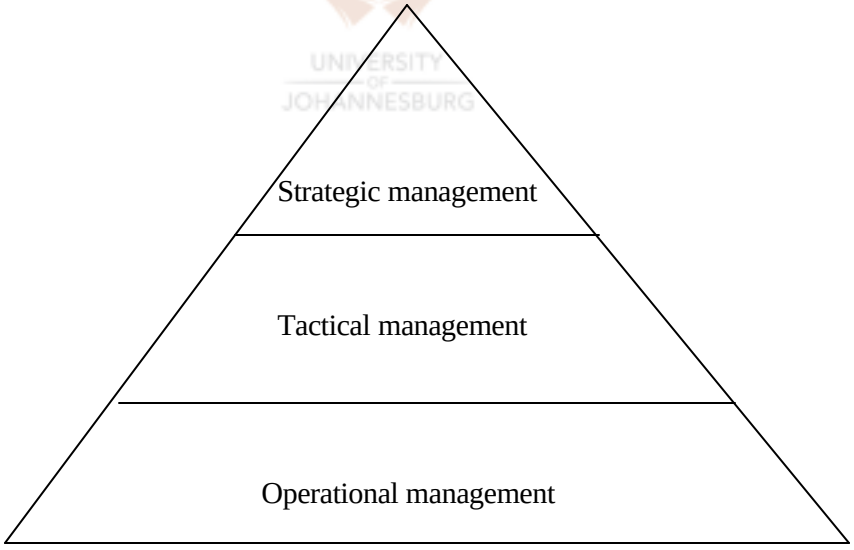
4.3.2.1 Management defined

Various definitions may be advanced as to who a manager is and what the concept of management entails.[104] For the purposes of this dissertation the definition as proffered by the Companies Act have been adopted. The term "manager" is defined by section 1(1) of the Companies Act[105] as meaning "any person who is a principal executive officer of the company for the time being, by whatever name he may be designated and whether or not he is a director."

4.3.2.2 Levels of management

Different levels of management exist within the organisation. [106] Within the context of information security governance it is important to observe these different levels, as only top level management will be held accountable for information security governance subsequent to the board of directors.

Three primary levels of management may be identified, namely:



[104] Smit and Cronje *Management Principles* (1992) 6 define management as: "…a process or series of activities that gives the necessary direction to an enterpise's resources so that its objectives can be achieved as productively as possible in the environment it functions." O'Brien (n 71) 356 views the concept of management as: "…a process of leadership involving the management functions of planning, organising and controlling."

[105] Act 61 of 1973.

[106] (n 71) 359.

(i) Strategic management[107]

The strategic level of management comprises of top management in the upper-level of the management hierarchy. The strategic management level is normally limited to the president and vice president of the organisation.[108] In general their decisions and actions have far reaching consequences and will have a long-term influence and impact on the organisation.[109]

Members of strategic management is responsible for:

(a) "Develop overall organisational goals, strategies, policies, and objectives through long-range strategic planning."[110] It should be kept in mind that although top-level management is responsible for the development of organisational strategy, objectives, goals and mission, it is not concerned with the actual implementation thereof;[111] and

(b) "Monitor the strategic performance of the organisation and its overall direction."[112]

(ii) Tactical management[113]

This level of management comprises of middle-level managers, who are responsible for implementing the visions of top level management.[114]

Their functions include amongst other things:

(a) "The development of short-and–medium range plans and budgets and specific policies, procedures, and objectives";[115]

---

107 Also known as the strategic planning level.
108 McLeod and Schell *Management Information Systems* (2001) 5.
109 ibid.
110 (n 71) 359.
111 (n 5) 72.
112 (n 71) 359.
113 Also refer to as the management control level. Examples of members of management that will fall within this level are regional managers, product directors and division heads.
114 ibid.
115 (n 71) 359.

(b) Procurement and assignment of resources; [116] and

(c) Performance measurement and monitoring of organisational departments, units and subdivisions. [117]

(iii) Operational management[118]

The operational management will comprise of lower-level management who receive their instructions from senior management in the form of strategic goals.[119]

Their functions include amongst other things:

(a) "Supervisory management develop short-range planning devices as production schedules"; [120]

(b) "Direct the use of resources and the performance of tasks according to established procedures and within budgets and schedules established for the work groups of the organisation";[121] and

(c) "They are responsible for accomplishing the plans specified by managers on upper levels."[122]

This dissertation will focus on strategic level management, as they may, along with the board, incur legal liability for non-compliance with information security governance.

---

116 ibid.
117 ibid.
118 Also referred to as the operational control level. Examples of managers who fall within the parameters of this level include department heads, supervisors, and project leaders.
119 (n 5) 72.
120 (n 71) 359.
121 ibid.
122 (n 108) 5.

4.3.2.3 Authority vested in management

Management is answerable to the board when performing their activities or executing decisions. Their accountability and powers differ from that of the board because "management does not work directly for owners, only the board does."[123] Management is furthermore not considered to be an organ of the organisation, it is a mere functionary.

4.3.2.4 Principal managerial activities[124]

Different management theories exist regarding the functions and activities management must perform.[125] The traditional view on management exist within the parameters of five activities, namely: [126]

(i) Planning

In its most simplistic form planning may be defined as "the method by which a person identifies key goals, and how to achieve them."[127] Planning is a management activity that enables the organisation to decide what to do before they do it.[128] Although it may be regarded as the first step in the management process, it cannot take place in isolation of other functions and/or activities. [129]

---

123 (n 11) 6.

124 These management functions/activities elaborate on a model build by Henri Fayol around 1914.

125 Some of the more influential theorists include: Weber; Jaques; Pfeiffer and Salancik; Fayol; Mintzberg; McGregor; Hertzberg; Hilmer and Donaldson; Strassman; Moltke. To gain more insight into their theories part "C" of Aalders and Hind *The IT Manager's Survival Guide* (2002) may be consulted.

126 It was contended by Fayol that all managers, irrespective of the level on which they operate would deal to a greater or lesser extend with these functions. Some writers are however of the opinion that there only exists four central activities which management must perform, they do not regard staff as one of these. Amongst these writers are Smit and Cronje (n 104) 4-5.

127 (n 5) 73.

128 (n 71) 538.

129 (n 104) 58.

What does the concept of planning embody?

(a) "The development of long-and-short range plans requiring the formulation of goals, objectives, strategies, policies and procedures and standards";[130] and
(b) "It identifies ways of attaining those goals as well as resources needed for the task."[131]

Planning occurs on different levels. Therefor different categories of planning are encountered, namely strategic planing, tactical planning, operational planning and long-and-short term planning. [132]

(ii) Organising

The second step in the management process is organising. "Organising involves developing a framework to indicate how personnel and materials should be employed to achieve the goals."[133]

(iii) Staff

The organisation needs to be equipped with the necessary resources, one of which would include skilled personnel. [134]

(iv) Directing

Directing entails "…getting and keeping management activities going, motivating and influencing personnel as well as communicating with and among personnel."[135]

---

130 (n 71) 356.
131 (n 104) 6.
132 (n 104) 56.
133 (n 104) 7.
134 ibid.
135 ibid.

(v) Controlling

Controlling is concerned with "…observing and measuring organisational performance and environmental activities of the organisation where necessary."[136]

4.3.2.5 Characteristics of effective managers

The traditional function of managers in the organisation have not been transformed by the onset of the information age, rather it has been supplemented and complimented by it. It is now expected of managers to become computer and information literate.[137] Computer literacy entails that management must have a basic understanding and knowledge of computers.[138] Information literacy entails that managers must understand how and why information is used within the organisation, what are the benefits delivered by information, and how it enables the organisation to reach its set goals and objectives.[139] Therefor managers need to realise the value of the organisation's information assets.

4.4 Information age challenges facing the board and management

(i) Information security is a relatively new concept to management.[140] Unlike other management disciplines like accounting, finance and production, information security does not have a "body of theories and practices in place" that have been tested, evaluated, proven and refined over time.[141]

(ii) Corporate values have witnessed a significant change. In the past we found that investors were mainly concerned with, and motivated by two primary factors,

---

136 (n 71) 356.
137 (n 108) 9.
138 ibid.
139 ibid.
140 The first computers were introduced into large firms in the late 1950's and 60's.
141 (n 86) 7.

namely: (i) "the company's profitability and cash flow"; and (ii) "its rate of growth."[142] The Internet and associated dot.com explosion have shifted this balance. Investors are now more concerned with growth than with profitability.[143] Therefor investors are willing to invest more and wait longer for their return on investment. They believe in the first-mover advantage.[144]

(iii) Because of the complexities associated and embedded in IT we find that the concept of an "IT specialist" represents some difficulties. At present it will be hard to find a general IT specialist, as the new trend amongst these professionals are to become IT subspecialists.[145] Therefor organisations will no longer be able to employ only one or two general IT specialists, yet it would be unrealistic to expect of organisations to attempt to employ specialists in every subdivision of IT. Consequently management must start looking at **outsourcing** as a viable option.[146]

Outsourcing: the advantages and disadvantages attached to external advice[147]

Outsourcing may be defined as "the decision to contract out part or all of the running of the computer systems to an outside organisation."[148] It may be viewed as "the process by which an in-house function is passed to an external service provider, usually to save money and to streamline the business."[149]

---

142 (n 39) 126.

143 ibid.

144 This believe entails that "those firms who can establish a strong identity on the Net…will show tremendous growth potential".

145 (n 86) 9.

146 For a discussion on a director's liability for outsourcing see chapter seven below.

147 At present numerous companies outsource security measures such as firewalls, intrusion detection services, vulnerability assessment, anti-virus management, and security intelligence. It is predicted that organisations will in the future turn to managed security services providers (MSSPs) for effective ways to deal with complex information security-related issues. For a comprehensive discussion on outsourcing, consult Lacity, Willcocks and Feeny "IT outsourcing: maximizing flexibility and control" (2001) *Harvard Business Review On the Business Value of IT* 2.

148 (n 5) 88.

149 Graham and Redman "Legal issues arising on an IT outsourcing" (14 March 2003) *NLJ Information Technology Supplement* 381.

The following reasons may be advanced why organisations are **reluctant** to employ consultants:

(a) The employment of a consultant might be viewed by some stakeholders as an "admission of failure";[150]

(b) Cost associated with contracting a consultant is very high;[151]

(c) Some consultants advocate "client-dependency," thereby making the organisation with which they contracted initially, and for a specific purpose, totally dependent on the services provided by the consultant.[152] The consultant would for instance keep on identifying and/or creating problems that must be addressed and that can only be addressed by him;

(d) Privacy and confidentiality concerns are highlighted whenever an organisation decides to outsource;[153] and

(e) It may furthermore be very difficult to decide which functions or operations to outsource, and which to keep in-house.[154]

Advantages offered by outsourcing

(a) Employees do not possess over the necessary skills and expertise, or there may be a shortage of staff, or both.[155] "Outsourcing provides access to a larger pool of talent";[156]

(b) Consultant usually possess over expert knowledge of the information security tools, products or mechanisms the organisation may wish to implement;

(c) Consultants give an objective view, whereas employees may have personal self-interest motivating their decisions and recommendations; and

---

150 (n 5) 85
151 ibid.
152 (n 5) 86.
153 (n 5) 88.
154 ibid.
155 ibid.
156 Pearlson *Managing and Using Information Systems* (2001) 178.

(d) Even though consultant's fees are high the cost attached to outsourcing may still be less than attempting to educate or train existing employees on a specific topic. [157] Worse still, the damage that may be inflicted by an uninformed employee will far outweigh the cost of outsourcing.

Steps that need to be taken in order to ensure outsourcing will be successful:

(a) Articulate clearly the outcome outsourcing must deliver; [158]

(b) Predetermine and gain certainty about the application, unit, function or system that is going to be outsourced; [159] and

(c) Conclude a comprehensive contract. [160]

The question may be asked what should be outsourced, and what should be kept in-house? It may be argued that if the IT operation provides the organisation with a strategic advantage, then it should be kept in-house. [161] However, if the IT operation does not provide a competitive advantage, thereby differentiating the organisation from its competitors, then this operation or function may be outsourced.

(iv) Intangible nature of benefits the organisation will receive. The traditional approach of the board is the evaluation of performance of the organisation, department or unit in rands and cents. [162] Unfortunately IT, and specifically information security offer intangible benefits that the board may never be able to successfully convert into monetary terms. A shift in the mindset of the board is therefor required whereby they compare the position of the organisation without

---

157 (n 5) 88.

158 Aalders and Hind *The IT Manager's Survival Guide* (2002) 158.

159 ibid.

160 ibid.

161 Lacity, Willcocks and Feeny "IT outsourcing: maximizing flexibility and control" (2001) *Harvard Business Review on the business value of IT* 2.

162 "The only benefit that count at the end of the day are monetary, that is to add profit… if you can't measure it, it does not exist." Grindley (n 18) 90; 197.

information security measures, to that of the organisation with these measures in place.

(v) Rules of competition have changed. Organisations are now competing on a global scale. The Internet is changing the way in which businesses compete.[163] Dot.com companies are not staying within the boundaries of their traditional sectors in which they might have operated in the real world.[164] Therefor companies are venturing into new markets, products and services they would never have considered before. [165]

Porter and Millar[166] identified three ways in which the information age affected the rules of competition:

(a) "It changed the industry structure, and in so doing, alters the rules of competition;

---

[163] (n 39) 128.

[164] ibid.

[165] New business models are emerging, unknown to the "traditional" business world. The following business models for the Internet may be identified:

(a) B-to-B Business-to-Business – targets sales and services primarily to other businesses;
(b) B-to-C Business-to-Consumer – targets sales and services primarily to consumers;
(c) B-to-E Business-to-Employees – companies that provide services other companies can use to interface with employees;
(d) B-to-G Business-to-Government – companies who sell the bulk of their goods and services to state, local, and national governments;
(e) C-to-C Consumer-to-Consumer – sites that primarily offer goods and services to assist consumers to interact; and
(f) Hybrid A combination of B-to-B and B-to-C models.

It is contended by Conger, Lawler and Finegold that these new models "place significant pressure on the way traditional firms are governed." Some practical examples of these new business models include:

(a) "Virtual markets, or business to business exchange – here thousands of buyers and sellers can come together;
(b) Name-your-own-price sites – where individuals can decide what they want to pay for a service or product, and the supplier then decides if they are willing to accept the offer;
(c) Heavily discounted or free products and services offered; and
(d) Smart shopping tools that do an automated search for the lowest price available on a particular good or service." Conger, Lawler and Finegold (n 39) 129.

[166] Porter and Millar "How information gives you competitive advantage" (July-August 1995) *Harvard Business Review* 150.

(b) It creates competitive advantages by giving companies new ways to outperform their rivals; and

(c) It spawns whole new businesses, often from within a company's existing operations."

Globalisation[167] therefor inevitably brings with it new and unknown adversaries. In order for organisations to not only remain competitive, but also to survive in general, organisations must become and remain flexible and able to adapt to the challenges and changes accompanying this new era.

(vi) A cultural gap exists. Although it is acknowledged that technological and managerial issues pose problems the biggest problem faced by directors is a lack of understanding.[168] The onus rests on each member of the board to educate himself/herself on information security governance.

Although the information age holds numerous challenges and obstacles it also has advantages:

(i) Boards are forced to educate themselves on technology related issues and become more susceptible to the information age and the challenges accompanying it; [169]

(ii) The board has access to more information than ever before. This will enable them to make more informed decisions; [170]

(iii) New business partners will be identified; [171]

(iv) The Internet exposes the organisation to new market opportunities never envisage before by the brick-and-morter organisation; [172] and

---

167 O'Brien (n 71) G 8 defines globalisation of organisations as: "…becoming a global enterprise by expanding into global markets, using global production facilities, forming alliances with global partners…".

168 (n 18) 114.

169 (n 39) 128.

170 ibid.

171 ibid.

172 ibid.

(v) The exchange of data occurs at a rapid speed with almost no monetary cost associated with it. [173]

4.5 Conclusion

From this discussion it should be clear that the board and top management are at present faced with a daunting task. The advent of the information age, the increased reliance on information technology and the Internet as a tool to conduct business, inevitably brings with it serious security consequences.[174] The activities and decisions of the board are being scrutinised by various stakeholders, including investors, the government and even the organisation's own employees.[175] This necessitates that the board must become proactive and educated on information technology, information security and other technology-related issues.[176]

At this point it is understandable that the board and management might feel discouraged, reluctant, and overall negative towards information security governance. They may feel as if the information age has placed an unnecessary heavy burden on them. But the truth of the matter is that boards do not have the luxury of deciding if they want to implement information security governance within their organisation. The development of this discipline is not a suggestion but a prerequisite for any organisation doing business by means of electronic communication systems in the information age. If information security is not governed within the organisation, directors can be held personally liable for non-compliance with their duty of due diligence.

In order to provide directors and top management with some form of motivation when developing and implementing information security governance the next chapter will make the business case for information security governance, by illuminating the business value of this discipline and indicating how it contributes to the bottom line.

---

173 ibid.
174 (n 39) xiv.
175 (n 39) xi.
176 ibid.