CHAPTER EIGHT: CONCLUSION

8.1 Research objectives

The objective of this dissertation was to outline the legal implications of information security governance by defining information security governance, identifying those entities who should concern themselves with the application of this discipline, how it should be applied, benefits that will be derived from it, and consequences of non-compliance.[1]

8.2 Scope

The research focused on public companies and private companies, who have to comply with information security governance in accordance with the King II report.[2] Although King II is only compulsory for listed companies, as have been reaffirmed by the JSE New Listing Requirements, private companies may find themselves being "forced" into compliance by means of the common law, peer pressure and media attention. [3] The research also took into account the ECT Act,[4] which dealt with specific technical security issues. [5]

Furthermore, the research was conducted with the aim of giving the reader a theoretical background to the discipline information security governance, while simultaneously incorporating the practical aspect thereof. By asserting the legal implications of information security governance a framework may be formulated that may be used for implementing this discipline within the organisation.[6] However, the reader should be

---

1 See Ch 1.
2 King Committee *King II Report on Corporate Governance 2002* (2002).
3 See Ch 3.3.5.
4 25 of 2002.
5 See Ch 2.7.
6 See Ch 6.

mindful of the fact that "in theory there is no difference between theory and practice. In practice there is. Theory works best in ideal laboratory settings. The real world involves design trade-offs, unseen variables, and imperfect implementations."[7] Therefor, the suggested seven-step framework should be viewed as a template relevant to any organisation, that still has to be customized and adapted to fulfill the needs of the specific organisation in which it is going to be applied.

8.3 Findings and recommendations

It has been established that information is one of the most important assets over which an organisation may possess.[8] Since most organisations have made the move from the physical world into cyberspace this asset has been under attack from a multitude of new fronts. Consequently, information security has propelled itself into the limelight as the preferred method to secure the organisation's information assets. However, because of the fact that information security is a complex, dynamic and multifaceted discipline of which no one component may be ignored, the effective governance of this discipline is pivotal for any organisation wishing to survive and prosper in the information age.[9]

Two entities that will be responsible for the governance of information security have been identified, namely the board of directors and top management.[10] Although they are the primary role-players in information security governance they generally have insufficient insight into the legal implications of information security governance. An understanding of these implications are however pivotal, especially for directors who may incur personally liable for failed information security.[11]

---

7 Schneier *Secrets and Lies* (2000) 8.
8 See Ch 1.
9 See Ch 2.
10 See Ch 4.3.
11 See Ch 7.

The King II report states, in no uncertain terms that ultimate responsibility for information security vests in the board of directors. [12] The ECT Act also contains specific provisions relating to technical information security. This newly-found focus on information security by South Africa, is in line with the approach taken by the rest of the international community. The international community is not only giving serious consideration to information security, and the governance thereof, but is increasingly demanding that those people responsible for information security (directors and top management) be held accountable for failed information security.

Ultimately it is expected of the board of directors and top management to take reasonable steps to secure their organisation's information assets. It is therefor concluded that the effective implementation of information security governance is dependent on two critical success factors. Firstly, the concept of information security governance must be embraced. Therefor, top management must become informed, and be committed to this discipline, and this commitment must cascade down to lower level employees. Ultimately this will result in a culture of security being fostered within the organisation. Secondly, information security must effectively be executed and implemented within the organisation. This would inevitably include the monitoring, maintenance and evaluations of this discipline on a regular basis.

To aid the board in discharging the multitude of onerous responsibilities and duties that this governance discipline places on them, the researcher **recommends** that:

(i) **An IT director should be appointed as a member of the board**. [13] The aim with this appointment is two-fold: firstly IT-related matters, including information security, will be elevated to boardroom-level, thereby eliminating the possibility that IT will be dealt with solely as a technological issue, ignoring the business side of it all-together; and secondly, the board and top management will have

[12] See Ch 6.3.2.5.
[13] See Ch 4.

access to a knowledgeable individual who they may approach with question, and for advice on IT-related issues; [14]

(ii) **An Information Security Strategy Committee should be established**. [15] This committee will focus its attention on the business value of information security governance, thereby ensuring that the maximum benefits are derived from this discipline. The functions of this committee include amongst other things, (a) the alignment of information security mission, goals and objectives with the overall organisational mission, goals, and objectives, thereby allowing information security to function, not only as a business supporter, but also enabler, and ultimately transformer; (ii) measuring the performance of information security within the organisation to ascertain if information security is delivering against expectations, and if not, investigate the reason for this. [16] Furthermore, performance measurement will aid security professionals in justifying future, current, and past investments in information security, as an effective performance measurement system will capture the illusive value of information security. Although numerous valuation methodologies exist, the researcher is of the opinion that corporate South Africa, like the rest of the world, will increasingly be looking at the balanced scorecard approach to performance measurement as a viable option; [17]

(iii) **An Executive Risk Management Committee should be established** that will aid the board in determining the radius of risk to information security in the organisation. [18] This committee will mainly concern itself with the subdiscipline information security risk management, and will be responsible for its development, implementation and monitoring thereof.

---

14 See Ch 4.
15 See Ch 5.4.
16 See Ch 5.
17 See Ch 5.3.6.
18 See Ch 6.3.2.

Included in the risk management concept, is the execution of risk assessment and risk mitigation processes.[19] After completion of the first leg of risk management, namely risk assessment, it is recommended that a Risk Assessment Report is compiled that will give the organisation a summarised overview of the most prevalent risks, threats and vulnerabilities facing the organisation, the motivation behind each, the likelihood of occurrence, and the estimated impact if the risk materialises, or a vulnerability is exploited.[20] The Risk Assessment Report will ultimately form part of a database that the organisation must construct. This database will provide invaluable information on risks, threats, and vulnerabilities the organisation has been faced with in the past. It will also serve as the basis on which to justify past, present, and future decisions and acts. Ultimately, it will act as proof that directors have fulfilled their duty of due diligence. This recommendation is in congruence with the King II report, which requires of organisations to systematically document the risk assessment process as well as the results delivered by this process and communicate this information to all relevant role-players. [21]

During the second leg of the risk management process, namely risk mitigation, top management will receive the Risk Assessment Report accompanied by recommendations on safeguards and control measures that should be implemented. [22] They will then have to decide: (a) whether or not they are going to act on the report; (b) determine if the risk should be deemed acceptable or unacceptable; and if a risk is deemed to be unacceptable (c) which safeguards and control measures should be implemented to reduce unacceptable risks to an acceptable level. Keep in mind that the implementation of safeguards and control measures are not mandatory, but optional. It is however recommended that if top management decided against the implementation of a recommended security

19 See Ch 6.3.2.
20 See Ch 6.3.2.
21 See Ch 6.3.2.
22 See Ch 6.3.2.

measures, this decision must be fully motivated and explained in a Risk Acceptance Report.

(iv) **Legal council must form part of both the Executive Committee for Security, as well as of the Security Team.**[23] The functions of the legal council would include: (a) the drafting of information security documentation in order to ensure that it is legally binding on employees; (b) the enforcement of security documentation which could result in termination of employment; (c) if the latter does occur assurance must be gained that the correct procedures are followed in order to avoid disputes in the future based on unfair dismissal and/or unfair discrimination; [24] (d) keep management informed of all new legislation and relevant regulations that will impact on the organisation's information security practices and procedures; (e) address issues pertaining to corporate and personal liability for failed information security, which would include holding those responsible for information security accountable, and prosecute those who violate security;

(v) Directors and top management will have to start looking at **outsourcing** as a viable option. [25] 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. 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, organisations should consider outsourcing some of their information security functions; and

---

23 See Ch 2.
24 See Ch 6.3.3.
25 See Ch 4.4.

(vi) Arguably, the most significant legal implication of information security governance is that directors may be held **personally liable for failed information security**. [26] Therefor, one of the main reasons why the governance of information security should have a prominent place on the board's agenda is because of the fact that if a director omits to take reasonable steps to secure the organisation's information assets he may incur personal liability. It is therefor recommended that directors educate themselves on the statutory and common law duties they owe to, not only to the organisation itself, but also to stakeholders of the organisation. Specifically, within the information security governance domain, they will have to give regard to the common law duty of care and skill/due diligence, as this duty will provide the basis on which a plaintiff (stakeholder) will be able to hold a defendant (organisation and director) personally liable for failed information security. [27] However, one of the biggest problems experienced with this common law duty is that no objective standard to measure compliance against have been developed.[28] In order to evaluate if a director has fulfilled this duty, it is recommended that an information security governance due diligence assessment be performed. A proactive strategy to information security governance will result in a tick in every box:

Information security:

- ☑ Is the responsibility of the board of directors;[29]
- ☑ Results in a consistent, integrated view across the organisation of the importance of information security; [30]
- ☑ Forms an integral part of the overall organisational structure;[31]

---

26 See Ch 7.
27 See Ch 7.
28 See Ch 7.3.2.
29 Appleby (ed) "Closing the gap: bringing boards into the IT equation" (August 2001) *Information Edge* Vol 7 number 7 2.
30 ibid.
31 ibid.

- ☑ Aligns information security mission, goals and objectives with organisational mission, goals and objectives;[32]
- ☑ Ensures that risks are quantified, understood and managed;[33]
- ☑ Directs and controls information security investments, opportunities, benefits and risks;[34]
- ☑ Adopts a balanced approach between all three components of information security, namely physical, technological and procedural security; [35]
- ☑ Provides a clear view of how much is spend, on what, and measure return on investment; [36] and
- ☑ Protects shareholder and stakeholder value.[37]

If there is not a tick in every box the organisation, and more importantly its board of directors may be judged irresponsible regarding the approach taken to information security governance. However, if there is a tick in every box the board of directors have taken reasonable steps to security the organisation's information assets, thereby fulfilling his duty of care and skill/due diligence. Consequently, even if a security breach or incident took place at a later stage he will still be able to escape liability.

It must however be realised that there is no such thing as a hundred percent secure environment. "Perfect security is unattainable at any price. The key is to determine the point of diminishing returns for an organisation's particular mission and geography."[38]

---

32 ibid.
33 ibid.
34 ibid.
35 ibid.
36 ibid.
37 ibid.
38 Appelgate, McFarlan and McKenney *Corporate Information Systems Management* (1999) 240.

Therefor, "rather than lulling themselves into a false sense of security, companies who wish to safeguard their proprietary information from prying eyes of trading partners and hackers would do well to take up the mantra: 'only the paranoid will survive'."[39]

8.4 Conclusion

While information security governance enspheres all aforementioned issues and topics discussed in this dissertation, it also transcends them all. The following citation best captures the demand for, and hidden danger embodied in the discipline information security governance:

> "Security, like risk, is a capacious concept, perilously capable of meaning all things to all comers. Like risk, security provokes strong emotions and licenses extraordinary exercise of power. But, whereas risk threatens, security promises. And in this power of promise what it cannot deliver lies a particular danger."[40]

Such is the essence of information security governance.

[39] Heske "Security 2001: As strong as the weakest link in the chain" (last visited 18 February 2002) http://www.computingsa.co.za/compsaarchive/2001/01/29/feature/fea01.htm3.

[40] Zedner "The concept of security: an agenda for comparative analysis" (March 2003) *Legal Studies* 176.