CHAPTER SEVEN:
LEGAL LIABILITY FOR INFORMATION SECURITY GOVERNANCE

7.1 Structure of chapter

> "There are no court cases as yet dealing with the issue of what a director or other officer would be expected to do in relation to e-security in order to discharge their statutory duties. It is, nevertheless likely that a Court would apply the duty to exercise care and diligence in such a way as to require a director or other officer to take reasonable steps to ensure that a corporation operating in an online environment has reasonable e-security policies and practices."[1]

This chapter will address the question whether or not this excerpt is an accurate reflection of the truth.

The general point of departure whenever contemplating instituting a legal action, would be to obtain certainty and clarity regarding the following issues:

(i) **Plaintiff:** Who is the person bringing the action/application, and is he/she entitled to do so?

(ii) **Defendant:** Against whom is this action brought? and

(iii) **Grounds:** On what ground(s) can this action be brought before the court?

Once these three initial questions have been answered, attention will be focused on the following questions:

(iv) **Duty:** Does the defendant have a duty to protect information and under what standard should that duty be evaluated?

---

[1] Fernon, McCullagh and McEniery "Board responsibility for protecting information assets" (last visited 26 November 2002) http://www.freehills.com 1.

(v) **Breach:** Did his/her act or failure to act fall short of acceptable standards and best practices?

(vi) **Causation:** Was the breach of the duty related to the damages/harm suffered by the plaintiff?

(vii) **Damages:** Did this action/omission cause the plaintiff to suffer quantifiable harm?; and

(viii) **Defenses:** What possible defenses may the defendant rely on?

The exposition of this chapter is therefor aimed at empowering directors and top management by assisting them in understanding the legal position surrounding liability for failed information security. This objective is achieved by taking a practical legal approach, much like the one a plaintiff would take when instituting an action for failed information security.

Outline of chapter:

Legal liability for failed information security centers around four questions:

(i) Who owes a duty of care?

(ii) To whom?

(iii) In respect of what damages? and

(iv) What are some of the possible defenses?

These four questions will be addressed in part three to seven hereafter.

It is concluded that the common law duty of care and skill is the most prevalent within the information security government domain, as this will be the ground on which a plaintiff (stakeholder) will be able to hold the defendant (organisation and director) personally liable. One of the biggest problems experienced with this common law duty is that no objective standard to measure compliance against have been developed. The researcher concludes that although this duty is to be found in most company law legislation around the world, and is acknowledged, recognised and enforced internationally, countries have been unsuccessful in formulating an objective test that can

be applied in practice. [2] It should furthermore be noted that the basis of an action for breach of a duty of care and skill is not to be found in the law of contract or delict. It is *sui generis*, therefor the duty has its own unique character.

Caveat: The use of inconsistent terminology in corporate law literature may confuse the reader. Therefor, the reader must be mindful of the fact that the concept of "due diligence" and the concept of "duty of care and skill" are indistinguishable. These two concepts embody exactly the same duty. The duty of due diligence in American company law is equivalent to the duty of care and skill found in other jurisdictions.

7.2 Introduction

The information age brought with it significant advances, changes and challenges, which inevitably resulted in the business environment becoming more complex. As a result of these changes and challenges an increase in, and more stringent application of the duty of care and skill may be observed. Fernon[3] comments that these changes "have significantly raised the bar as far as director's duties are concerned."

The impact of the increased demand for this duty, combined with the austerity with which it is enforced should be a growing concern for directors, as they may now be held personally liable if an information security incident occurred as a result of their "failure to adequately secure their company's computer systems, or if information of a proprietary

---

[2] The reader will observe that reference is made quite frequently to English law. The reason for this being that the South African Companies Act 61 of 1973 is based to a great extend on English company law. "Many of the rules of the English common law of companies were readily accepted by our courts and introduced in South African law with little or no modification." Consequently, "…in cases where no guidance can be found in our common law, for the very reason that the company as we know it was taken over from English law, our courts have drawn from the experience of English law on the point in issue, and tended to follow the English precedents, if such an approach was justified…" Cilliers, Benade, Henning, Du Plessis, Delport, De Koker and Pretorius *Corporate Law* (2000) 19.

[3] (n 1) 2.

or sensitive nature is tampered with or stolen."[4] Therefor, in the information age, the scope of a directors responsibility will be extended to include the development, implementation and enforcement of an effective information security governance discipline. [5] Keep in mind this discipline will not eliminate the possibility of legal liability, but it will reduce it considerably. [6]

As stated earlier, legal liability for failed information security evolves around four main questions. Therefor, when wanting to institute an action for failure to take reasonable steps to secure the organisation's information assets, clarity must be obtained regarding the following questions: (i) who owes a duty of care? (ii) to whom? (iii) in respect of what damages? and (iv) what are some of the possible defenses? The remainder of this chapter will therefor be dedicated to answering these questions.

7.3 Identification of the defendant - Who owes a duty of care?

The first question "who owes a duty of care?" may further be subdivided into two questions:

(i) Who owes this duty? and

(ii) What does this duty entail?

7.3.1 Who owes a duty of care and skill?

A legal means must be found to hold those people responsible for information security accountable.

In chapter four two entities, namely the board of directors and top management, were identified as being responsible for information security governance. Consequently it

---

4 Gadens lawyers "E-commerce update: IT security: a director's challenge" (last visited 21 February 2002) http://www.gadens.com.au 1.

5 ibid.

6 ibid.

follows that they would ultimately also be held accountable for failed information security. [7]

Recent case law in the United States of America suggests that the risk associated with negligent information security will result in an explosion of lawsuits in the very near future. [8] The precedent have been set in cases such as *C.I. Host v Exodus (CITE)* and *Staples Inc. v Anonymous (CITE)* [9] where the tendency amongst plaintiffs are not to sue the hackers, but rather the organisation itself. This could ultimately result in liability of directors for breach of their duty of care and skill owed to the stakeholders of the organisation, as well as to the organisation itself. [10] This new trend is a direct result of the realisation by plaintiffs that hackers usually do not have "deep pockets," but organisations, especially those who want to protect their reputation and share price, do. They are willing to pay large sums of money to keep the case out of the court, and more importantly, out of the press.

The essence of legal liability of directors for information security may be captured by the following quote "…all the potential risks faced by the company and by its management in the end distil down to one essential element – the obligation to take reasonable steps to prevent an [IT] security breach...". [11]

Therefor, there is only question that should be asked concerning legal liability for information security "…can evidence be produced to show that the defendant (director)

---

7 A clear distinction should be drawn between the board's internal and external function and role within the organisation: (i) Internally: the board of directors are considered to be organs of the organisation. Consequently, "(w)hen an organ of the company acts it is for all practical purposes the company itself which acts – for certain purposes the organ *is* then *the company*"; and (ii) Externally: "(t)he legal position of a director or the board of directors should be explained with reference to the law of agency." Consequently, "(s)uch agents have no powers other than those conferred on them by the articles and can only bind their principal, the company, within the extend of their authority." Exceptions to this general rule does however exist, specifically when dealing with delictual and criminal matters. Cilliers, Benade, Henning, Du Plessis, Delport, De Koker and Pretorius *Corporate Law* (2000) 84; 117.

8 Christensen "Due diligence in infosec" (last visited 24 July 2003) http://www.health-privacy.org/due.diligence.3.htm 1.

9 ibid.

10 See also *FirstNet v Nike (CITE)* and *Metallica v John Does (CITE).*

11 (n 1) 3.

did not fulfill his or her duty of care and skill…?"[12] Consequently, regardless of what type of information security incident has occurred, be it theft of information or data; breach of privacy; industrial espionage or social engineering, a director will be held liable on the common law ground of duty of care and skill if he did not take reasonable steps to secure the information.

It is contended by Donn[13] that directors and top management alike are making a fundamental mistake when they view their function within the organisation as that of being risk reduction. "Our objective of risk reduction is the wrong basis for information security. It should be due diligence."[14]

7.3.2 What does the duty of care and skill entail?

From the preceding it should be clear that directors can be held liable for failed information security on the ground of non-compliance with their duty of care and skill/due diligence. The term "care and skill / due diligence" is however used impudently whenever reference is made to liability for failed information security without due consideration being given to what this duty entails. What follows is a brief discussion of what the duty of care and skill entails.[15]

(i) Duty of care and skill – a comparative analysis

The practice of placing directors under a duty of care and skill is found in company law legislation across the world.

---

12 Weiler "Decision support: you can't outsource liability for security" (last visited 6 September 2002) http://www. informationweek.com/story/IWK20020822S0003 1.

13 Donn "Risk management vs due diligence" (last visited 26 August 2002) http://www.csoonline.com/read/040103/letters.html 2.

14 ibid.

15 Some writers draw a distinction between duty of care and standard of care. The former is seen as the obligation owed to stakeholders of the organisation, whereas the latter is seen as "…what others in the same industry and of the same size are doing…" Symantec "Top management's perspective on security" (last visited 24 July 2003) http://www.symantec.com 4.

(a) American perspective[16]

In the United States of America directors must adhere to the **duty of diligence**.[17] In order to discharge this duty it is expected of directors and top management to have an effective compliance program in place.[18]

The following activities would be inherent to a compliance program:

(a) "Establish policies, procedures and standards to guide the workforce;

(b) Appoint a high-level manager to oversee compliance with the policies, procedures and standards;

(c) Exercise due care when granting discretionary authority to employees;

(d) Ensure that compliance policies are being carried out;

(e) Communicate the standards and procedures to all employees;

---

[16] The duty of due diligence in American company law may be equated to the duty of care and skill found in other jurisdictions. The main difference between the English and American duty of care and skill is the point of origin. The former's fiduciary duties evolved from principles found being placed upon trustees, whereas the latter never ventured into trust law, but rather developed from "common law rules governing agent's implied contractual duties of care and skill and the ability in torts of persons who undertake to provide services, whether under a contract, or not, if they cause loss by their negligence…". It would appear as if the American courts imposed a heavier duty of care and skill than the English courts. American courts deal with a director's duty of care and skill in one of two ways, namely: (i) applying stricter rules than the English courts; or (ii) following the same rules as the English courts. An example of where the former approach was used is *Hun v Carey* (1880) where the court held: "… one who voluntarily takes the position of director, and invites confidence in that relationship, undertakes, like a mandatory [an agent] with those whom he represents or for whom he act, that he possess at least ordinary knowledge and skill, and that he will bring them to bear in the discharge of his duties…The director's conduct was not a mere error of judgement…it was a case of improvidence, of reckless unreasonable extravagance, in which [the directors] failed in that measure of reasonable prudence, care and skill which the law requires" *Hun v Carey* (1880) 83. The second approach was adopted in *Barnes v Andrews* (1924) in which Hand J stated: "I cannot agree with the language of *Hun v Carey* that in effect [a director gives] an implied warranty of any special fitness [for his position]. Directors are not specialists like lawyers or doctors. They must have good sense; perhaps they must have an acquaintance with affairs; but they need not – indeed perhaps they should not – have technical talent. They are the general advisors of the business, and if they faithfully give such ability as they have to their charge, it would not be lawful to hold them liable" *Barnes v Andrews* (1924) 630. Keep in mind that the judge was not speaking about full time directors. It should be observed that in America a managing director is known as the president of the company Pennington *Director's Personal Liability* (1987) 88; 90. Furthermore, in America the duty of care that the board owes to the organisation and its stakeholders are of such great importance that it even extends to board members of non-profit organisations Spitzer "Right from the start: guidelines for not-for-profit board members" (last visited 24 July 2003) www.oag.state.ny.us/ charities/charities.html 3.

[17] The duty of diligence requires of directors to " …make business decisions on an informed basis, and act in good faith and with a honest believe that their actions were taken to serve the best interest of the corporation…" Cilliers, Benade, Henning, Du Plessis, Delport, De Koker and Pretorius *Corporate Law* (2000) 8.

[18] Peltier *Information Security policies, Procedures, and Standards* (2002) 24.

(f) Enforce the policies, standards, and procedures consistently through appropriate disciplinary measures; and

(g) Implement procedures for corrections and modification in case of violations."[19]

If a director is facing possible legal liability due to mismanagement or an alleged breach of his duty, the **business judgement rule** will abet him. The business judgement rule provides that "…courts should not examine the quality of the directors' business decisions, but only the procedures followed in reaching that decision, when determining the directors liability...".[20]

The purpose of the business judgement rule is to afford directors some protection against potential legal liability when making a *bona fide* decision, which later turns out to be "ill-advised."[21] The business judgement rule will not afford directors protection if they are (i) negligent, or (ii) unconsidered.[22] Therefor, under American law directors will lose the protection afforded by this rule if gross negligence can be proved.[23]

(b) United Kingdom perspective

Under the Companies Act 1985 of the United Kingdom directors are placed under the **duty of care and skill.** In order to discharge this duty it is expected of directors, when carrying out their duties as directors, to exercise such a degree of **care and skill**, as might reasonably be expected from someone of their ability and experience.[24]

---

19 Tipton and Krause *Information Security Management Handbook* Vol 3 (2002) 360.

20 Anderson "Protecting data by implementing a well-defined security policy" (last visited 25 August 2002) http://www.sans.org 122.

21 Marks and Tremaine "Director, trustee, and officer liability for information security" (last visited 24 July 2003) http://www.cio.com 6.

22 ibid.

23 *Kahn v MSB Bancorp Inc* (1998) WL 409355 (Del. Ch).

24 The duty of care and skill entails the following: "…directors are required to exercise a degree of skill and care that may reasonably be expected from someone in their position, albeit commensurate with their own knowledge and experience...". It is acknowledged that there is no objective standard to measure compliance with this duty, and therefor surrounding circumstances must be taken into account. Unknown "Director's responsibilities – a guide" (last visited 21 July 2003) http://www.thompson231.freeserve. co.uk/DirResp.html 4.

The starting point of exposition to any discussion on the duty of care and skill is found in English case law in the form of ***Re City Equitable Fire Insurance Co.***[25] This case is earmarked as being the *locus classicus* on the duty of care and skill, as is evident from the fact that courts at present still refer to this case when contemplating what the duty of care and skill entails.

This case reflects the traditional approach taken by the courts to this duty. It defined a director's duties in terms of three propositions:

(1) "A director need not exhibit in the performance of his duties a greater degree of skill than may be expected from a person of his knowledge and experience [26] **(skill);**[27]

(2) A director is not bound to give continuous attention to the affairs of his company[28] **(diligence);**[29] and

(3) In respect of all duties that, having regard to the exigencies of business, and the articles of associations, may probably be left to some other official, the director is, in the absence of grounds for suspicion justified in trusting that official to perform such duties honestly" **(reasonable care)** (own emphasis). [30]

25 (1925) Ch 407.
26 (n 25) 428.
27 It is evident from the first proposition that the court did not endeavor to develop an objective standard for a reasonable director. Furthermore this proposition resulted in the assumption that a director could only be held liable if gross negligence was present. Birds, Ferran and Villiers (ed) *Boyle & Bird's Company Law* (1995) 483.
28 (n 25) 429.
29 The duty of diligence does however involve much more than the mere attendance of a meeting, as is evident from the decision in *Daniels v Anderson* (1995) 16 ACSR 607, in which the court held: "…in our opinion the responsibilities of directors require that they take reasonable steps to place themselves in the position to guide and monitor the management of the company…" *Daniels v Anderson* (1995) 16 ACSR 664.
30 (n 25) 429.

(c) South African perspective

Fiduciary duty of care and skill

In South African law a director is placed under a **fiduciary duty** to **act with reasonable care and skill**.[31]

Fiduciary duties have their roots in the common law, and may be regarded as one of the most important duties to be found in the common law. Directors find themselves in a fiduciary relationship to their companies. [32] A fiduciary relationship will exist when "…he controls the assets of another or holds the power to act on behalf of another...".[33] This duty may be defined as requiring of the director to "…exercise his power *bona fide* and for the benefit of the company and to display reasonable care and skill in carrying out his office...".[34] It is important to bear in mind that a director cannot be released from the fiduciary duty he owes the company, be it by way of the articles,[35] a contract, or in any other way.[36]

The basis of legal liability for breach of a fiduciary duty is neither to be found in the law of delict, nor in contract law. [37] It is *sui generis.*[38] Furthermore, breach of a fiduciary duty may result in criminal liable.[39]

The importance of the fiduciary duty is emphasised by the fact that the King II report expressly makes reference to this duty. It states: "…the underlying principle of the King

---

31 Cilliers, Benade, Henning, Du Plessis, Delport, De Koker and Pretorius *Corporate Law* (2000) 147.
32 (n 31) 139.
33 ibid.
34 ibid.
35 Articles of association is defined by the Companies Act, section 1, as being "…in relation to a company, means the articles of association of that company for time being in force, and includes any provision, in so far as it applies in respect of that company, set out in Table A or Table B in Schedule 1…"
36 (n 31) 139-140.
37 (n 31) 141.
38 The fiduciary duty is said to be *sui generis* (unique/peculiar to itself), as it can not be classified under any one of the "traditional" legal categories, for instance, public law or private law.
39 (n31) 141.

Code is that directors should act not just in accordance with the letter of the law, but also in the spirit of their fiduciary duties…".[40] The report therefor scrutinises the role of the board of directors and gives specific consideration to their fiduciary duties.[41]

As stated earlier, in South African law a director is placed under a fiduciary duty to **act with reasonable care and skill.**[42] Certain difficulties are however experienced with this duty. Although the term "care" poses limited problems, as it may be determined objectively, the requirement of skill offers substantial problems, as it requires a very subjective approach. The importance of this duty lies in the fact that within the information security governance domain this duty will ultimately form the basis on which a plaintiff will be able to hold a director liable for non-compliance with the discipline information security governance.

South African courts have attempted to lay down general guidelines for the duty of care and skill. In *Fisheries Development Corporation of SA Ltd v Jorgensen*[43] Margo J highlighted three important aspects of this duty:

(a) A direct correlation between the extend of a director's duty of care and skill, and the nature of the company business may be observed;[44]

(b) A director's actions and decisions will be compared to that of a reasonable director. Therefor:

> "(a) director is not required to have special business acumen or expertise, or singular ability, or intelligence or even experience in the business of the

---

40 King Committee *King II Report on Corporate Governance 2002* (2002) 4.

41 Under the common law a director is required to act *bona fide*, in the best interest of the organisation, and with the care and skill one may expect from a person with his qualifications and experience.

42 (n 31) 147.

43 1980 4 SA 156 (W). A definite overlap may be observed between the three propositions as advanced by the court in *Re City Equitable Fire Insurance Co* and the *Fisheries Development Corporation of SA Ltd v Jorgensen* case 1980 4 SA 156 (W). It is interesting to observe that 55 years later the court did not attempt to augment these propositions, it would rather appear as if the court imitated them. Furthermore, it should be kept in mind that both these cases were concerned with the duty of care and skill in the physical world. They did not contemplate the extend or impact of this duty in cyberspace.

44 (n 31) 147.

company. He is however expected to exercise the care which can reasonably be expected of a person with his knowledge and experience"[45]; and

(c) Directors are allowed to delegate some of their functions and duties, but must still "…give it due consideration and exercise his own judgement accordingly...". [46]

Consequently, at present a pragmatic, case by case approach is followed by the South African courts. [47]

Other countries that have also made specific provision for this duty include: New Zealand, Austria, Greece, Norway, Spain, Canada, Luxembourg and Italy. [48]

The common denominator amongst all of these countries is that none of them have been successful in formulating an objective standard against which to measure compliance with this duty. Tests that have crystalised are still very subjective in nature. Notwithstanding this, it is, from a director's perspective, of pivotal importance to gain some insight, clarity and certainty regarding the nature of this duty, as this will form the basis of any legal action brought against him for purposes of information security governance.

(ii) Evolution of the duty of care

It may be observed from case law that the duty of care and skill may be equated to the shift of a pendulum that tends to oscillate between pro-plaintiff and pro-defendant attitudes over time. [49] In the 19th century and early parts of the 20th century, a relatively

45 (n 31) 148.
46 ibid.
47 Jones "The scope of professional liability – the professional's duty to third parties" (16 April 1999) http://www.cio.com 2-3.
48 For a more detailed discussion on how these countries apply the duty of care and skill consult Campbell and Campbell (ed) *International Liability of Corporate Directors* (1993) 490.
49 (n 47) 22.

low standard of care and skill was required of directors.[50] This approach was justified because directors were not regarded as being "professional" company directors. [51] They performed their functions on a part-time basis. Therefor, the elevation of part-time directors to full-time professional directors were, at that stage never envisioned. However, with the appointment of full-time directors, combined with the advent of the information age, and an increase in the complexities associated with the business and technological environment, the duty of care and skill is, at present being applied more strictly. Pennington[52] observes that:

> "…because he is better equip to pursue business opportunities on behalf of the company and far better informed about current matters than his nineteenth century counterpart, it would be surprising if the courts did not require him to show a higher level of attention, inquisitiveness and perception and to react more speedily and decisively to business situations than the case law of the nineteenth century would suggest is adequate…".

Although most authorities still refer to the propositions found in *Re City Equitable Fire Insurance Co*[53] there is a definite "move towards a more objective and thus demanding standard of care and skill for company directors." [54] Therefor a tendency amongst the courts to impose a higher standard of care and skill have come to the fore in recent years.[55]

In *Commonwealth Bank of Australia v Friedrich*[56] Tadgell J observed that the liability of directors have increased as the business environment in which they function becomes more complex. He goes on to observe:

> "…as the complexity of commerce has gradually intensified (for better or for worse) the community has of necessity come to expect more than formerly from directors whose task it is to govern the affairs of the companies to which large sums of money are

---

50 Birds, Fernan and Villiers (ed) *Boyle & bird's Company Law* (1995) 483.
51 ibid.
52 *Director's Personal Liability* (1987) 88; 90.
53 (n 25).
54 (n 50) 484.
55 (n 50) 485. See *Dorchester Finance Co. Ltd. v Stebbing* (1989) BCLR 498.
56 (1991) 5 ACSR 115.

> committed by way of equity capital or loan. In response, the parliament and the courts have found it necessary in legislation and litigation to refer to the demands made on directors in more exacting terms than formerly, and the standard of capability required of them has correspondingly increased. In particular, the stage has been reached when a director is expected to be capable of understanding his company's affairs to the extend of actually reaching a reasonably informed opinion of its financial capacity… I think it follows that he is required by law to be capable of keeping abreast of the company's affairs, and sufficiently abreast of them to act appropriately if there are reasonable grounds to expect that the company will not be able to pay all its debts in due cause as expected…".[57]

Consequently, it may be argued that the advances, changes and challenges brought about by the information age have increased the degree of care and skill directors are expected to exhibit.

After establishing who owes a duty of care and what this duty entails, the next question that may be asked is to whom such a duty is owed?

7.4 Identification of plaintiff(s) - Who are the plaintiffs?

From the preceding it would appear as if the duty of care and skill is very broad and onerous. It should however be kept in mind that directors do not owe this duty to everyone.[58] The board owes this duty of care and skill/due diligence only to stakeholders. Therefor it follows that if a duty of care is not owed to a plaintiff, no liability will arise.[59] As was decided in the Australian High Court "…the duty of care is owed to those with whom the person has a special relationship...".[60] Still the scope of persons qualifying as plaintiffs have been broadened when compared to the situation in the past. In the past the only people who would qualify as being plaintiffs would be shareholders and the owners of the company. Now King II broadens the scope of liability by recommending that

---

57 (n 56) 126.
58 *Modbury Tri*angle Shopping Center Pty Ltd v Anzil (2000) 176 ALR 411.
59 (n 47) 2.
60 (n 58) 411.

directors should be answerable to all stakeholders. [61] Consequently, specific regard has to be given to the interest and expectation of stakeholders.

The **onus/burden of proof** will rest on the plaintiff to produce evidence to show that the defendant (director) did not fulfill his or her duty of care and skill.[62]

Therefor the plaintiff will have to proof the following:

(i) That the defendant owed a duty of care to the plaintiff;[63]
(Did the defendant have a responsibility to protect the information?)

(ii) That the defendant breached that duty; [64]
(Can evidence be produced to show that he did not fulfill this duty?)

(iii) That the plaintiff suffered a legally recognizable injury; [65] and
(Was damage in the form of quantifiable harm suffered by the plaintiff ?)

(iv) That the defendant's breach caused the plaintiff's injury. [66]
(Causation - Is the breach of the duty close enough in relation to the damage suffered to be considered the primary cause thereof?)

---

61 The first King report defined stakeholders as: "..any person, entity or interest group that has some association with the company… There are three classes of stakeholders: shareholders, parties who contract with the company and parties who have a non-contractual nexus with the company. An example of a contracting party is the employee and a non-contracting party is the State...". King II defines stakeholders as: "…the community in which the company operates, its customers, its employees and its suppliers…The relationship between a company and these stakeholders is either contractual or non-contractual…".

62 (n 12) 1.

63 Miller and Jentz *Law for E-commerce* (2002) 86-87.

64 ibid.

65 ibid.

66 ibid.

7.5 Possible defense(s) at the disposal of the defendant

The only defense to such an allegation would be to proof that the director took reasonable steps to prevent the information security incident/breach from occurring, and that he acted honestly and in the circumstances ought to be excused.[67] Therefor it is required of directors to show due diligence (fulfillment of their duty of care and skill) through compliance with information security standards and best practices.

The question may therefore be asked: how does a director reduce his/her chances of being held liable for non-compliance with his/her duty of care and skill? Within the information security domain this question may be reformulated to ask: how does a director escape legal liability for failed information security?

7.5.1 Limiting the scope of liability [68]

(What is expected of the board to discharge this duty?)

In general the directors must have regard to the following four principles/guidelines to escape liability for a breach of the duty of care and skill:

(i) "A director should acquire at least a **rudimentary understanding** of the **business** of the corporation;

(ii) Directors are under a continuing obligation to **keep informed** about the activities of the corporation;

---

67 Unknown "Director's responsibilities – a guide" (last visited 24 July 2003) http://www.thompson231.freeserve.co.uk/DirResp.html 8.

68 Directors might feel tempted to outsource their information security with the expectation that they are also outsourcing responsibility therefor. This assumption is however incorrect. Although an increasing number of organisations are turning to outsourcing to solve their security problems it should be realised that outsourcing relieves neither the organisation, nor the directors of their liability for information security. "While this [outsourcing] relieves them of the burden of managing systems in-house, it doesn't take away a company's liability if there is a security breach." Consequently, directors must be mindful of the fact that they are not "outsourcing liability" Weiler (n 12) 2. For a comprehensive discussion on outsourcing see chapter four above.

(iii) Directorial management does not require a detailed inspection of the day to day activities, but rather a general **monitoring** of **corporate affairs** and **policies;**"[69] and

(iv) Generally, the standard directors must meet is to **act as carefully as they would have** acted under the same circumstances **if they were acting on their own behalf**" (own emphasis).[70]

Applying these principles/guidelines to the information security arena it would be expected of the organisation and directors alike to consider and gain assurance of the following:

(i) Boards and top management will have to educate themselves on what the discipline information security governance entails. This would inevitably require of them to understand why information security needs to be governed in the first place;[71]

(ii) Undertake a review of information security measures (physical, technical as well as procedural) currently employed by the organisation; [72]

(iii) Perimeter network security posture;[73]

(iv) Internal network security posture;[74]

(v) Organisational information security procedures and practices;[75]

(vi) Physical security posture;[76]

(vii) Establish an information security committee; [77]

(viii) Have a business continuity plan in place;

(ix) Adopt internationally recognised standards that will validate due diligence;[78]

(x) Comply with information security best practice; [79]

---

69 These principles were advanced in *Francis v United Jersey Bank* by Pollock J (n 48) 821-823.

70 (n 48) 121.

71 Symantec "Top management's perspective on security" (last visited 24 July 2003) http://www.symantec.com 4.

72 (n 1) 4.

73 Unknown "Information security due diligence assessment" (last visited 24 July 2003) http://www.technicaldefense.com/services.shtml 1.

74 ibid.

75 ibid.

76 ibid.

77 ibid.

78 (n 8) 1.

79 ibid.

(xi) Benchmark organisations information security against that of others in the same industry;[80]

(xii) Evaluate and oversee the overall risk management process, which encompasses risk assessment as well as risk mitigation; [81]

(xiii) Development and implementation of information security policies, procedures, standards and guidelines;[82]

(xiv) Provide information security awareness and training programs to all employees; [83] and

(xv) Review information security practices of the organisation on a continuous basis. [84]

If a director can successfully indicate that all of the above are in place it would validate due diligence.

It should be observed that the above-mentioned principles/guidelines will all be addressed by the implementation of the recommended seven-step plan, as set out in the previous chapter. It is therefor submitted that a director would have fulfilled his duty of care and skill/due diligence if he complied with the implementation requirements as set out in chapter six above.

7.5.2 Four pillar framework for information security

The aforementioned guidelines may be summarised and assimilated into a usable, practical, four pillar framework. This **framework for information security** may be advanced to aid the board in addressing key elements of their duty of care:[85]

---

80 (n 71) 4.

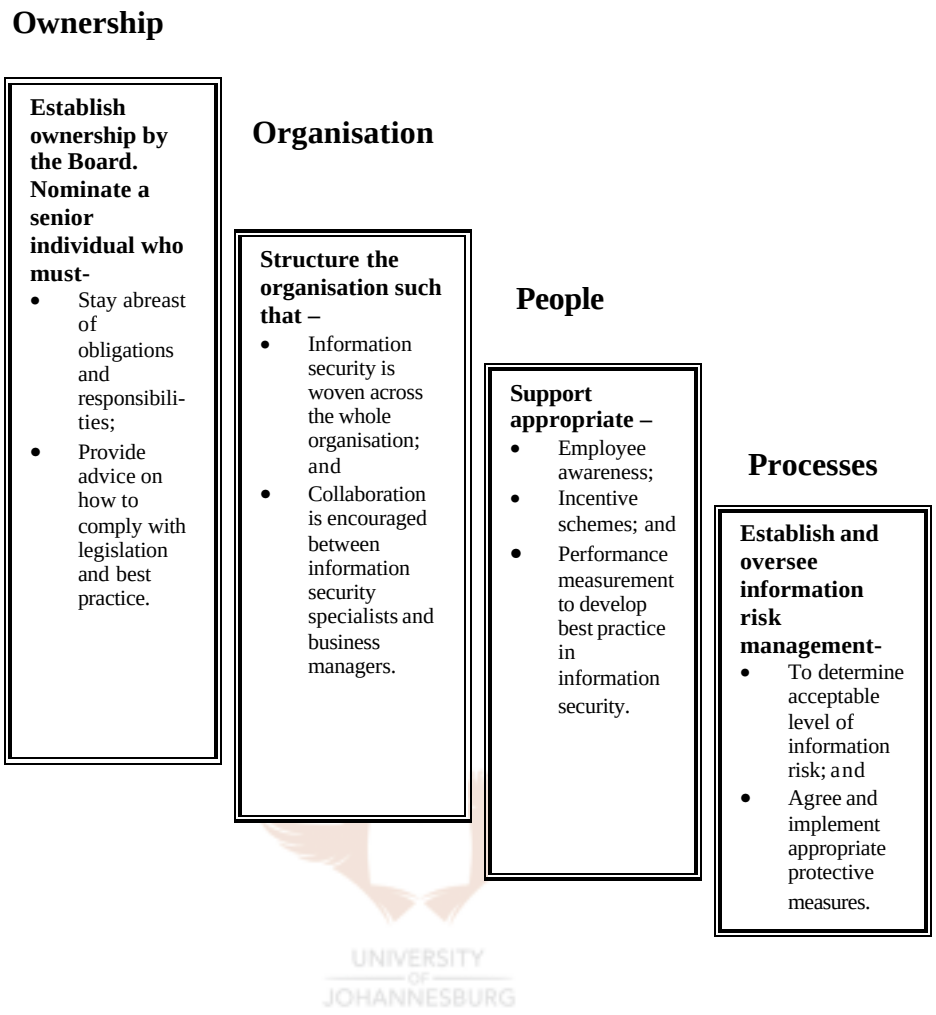
81 Zamorski "Security standards for customer information" (last visited 24 July 2002) http://www.fdic.gov/news/ news/financial/2001/fil0122.html 1.

82 ibid.

83 (n 1) 4.

84 (n 81) 1.

85 IAAC "Information assurance guidelines for boards and senior managers" (last visited 24 July 2002) http://wwwiaac.org.uk 3.



7.6 Court's viewpoint on due diligence in information security

In **Australia** the courts are of the opinion that:

> "…the question whether a director has exercised a reasonable degree of care and diligence can only be answered by balancing the foreseeable risk of harm against the potential benefits that could reasonably be expected to accrue to the company from the conduct in question...".[86]

Within in the information security arena this "test" may be reformulated as:

> "…if there is a foreseeable risk of loss to the company resulting from an [information] security breach, and the benefit likely to be gained from not adequately addressing that risk is low, then a

[86] *Vrisakis v ASC* (1993) 11 ACSR 162; 212.

director who does not adequately address that risk does not act with the requisite care and diligence…". [87]

If the organisation is presented with a situation where information security incidents have occurred in the past, and directors still do not apply the necessary care and skill, it might be argued that an even heavier burden will be placed on those directors, as they should have foreseen the possibility of another incident occurring.[88]

Therefor, when judging whether or not director have fulfilled against their duty of care and skill/due diligence the "current and sustainable information security posture" will be evaluated,[89] thereby assessing if any hiatus exist between acceptable standards and best practices, and the organisation's security posture. [90]

This would include launching an investigation into, amongst other things:

(i) The existence, scope and execution of:

(a) The risk management program to determine the radius of risk to information security in the organisation;

(b) Information security policies, standards, procedures and guidelines of the organisation; [91] and

(c) The organisation's information security awareness and training program. [92]

---

87 (n 4) 3.

88 *Mistmorn Pty Ltd(In Liq) v Yasseen* (1996) 21 ACSR in which this principle was applied. In this case directors were held to be in breach of their duty of care and skill. The court held that because of the fact that the directors had knowledge of previous thefts, and still omitted to take out insurance, they were in breach of their duty of care and skill owned to the company. Although this is an example occurring in the tangible/physical world, it is contended by the researcher that the courts can use their discretion to extend this duty to cyberspace.

89 Technical Defense Inc "Information security due diligence assessment" (last visited 24 July 2003) http://www. technicaldefense.com/services.shtml 1.

90 (n 8) 2.

91 (n 89) 1.

92 ibid.

(ii) How the organisation's information security practices compare to that of internationally accepted best practices for information security; [93]

(iii) To what extend the organisation benchmark itself against industry leaders and organisations in similar fields;[94] and

(iv) To what extend all three components of information security (physical; technical and procedural security) have been implemented, and the question whether or not they all enjoy the same level of attention and degree of importance. [95]

Keep in mind that "…anyone becoming a director for the first time should appreciate that claiming ignorance of a director's duties and responsibilities because one is 'new to the job' may well not be an acceptable defense if things go wrong…". [96] Similarly, it should follow that directors will not be ably to rely on their own ignorance of information security by merely stating that it is a new and unexplored field in the business environment of which they have limited knowledge. Furthermore, even if organisations decide to outsource their information security, liability and responsibility for information security can never be outsourced.[97]

7.7 Voluntary assumption of responsibility

An additional ground of legal liability for failed information security may be identified. It is contended that the plaintiff will have recourse to the law of delict, by using the English law principle of voluntary assumption of responsibility.

It is submitted that by accepting the office of director a person has voluntary assumed responsibility. This is an emerging concept in the English law that is applied especially

93 ibid.
94 (n 13) 2.
95 ibid.
96 ibid.
97 (n 12) 2.

when dealing with professional people such as attorneys and auditors. It is submitted that the same should apply to directors. By accepting his office a director has:

> "…promised the company that he or she had the skills of a reasonable competent person in his or her category of appointment and that he or she acts with reasonable care, diligence and skill...".[98]

The plaintiff (stakeholder) will argue that "…the defendant has 'assumed responsibility' towards them to take reasonable care to protect them from the loss that has occurred…".[99]

The origin of the principles underlying voluntary assumption of responsibility may be traced back to the English law case of *Hedley Byrne & Co Ltd v Heller & Partners Ltd.*[100] Although this case dealt specifically with liability for statements made, in *Henderson v Merrett Syndicates Ltd*[101] the court was of the opinion that voluntary assumption of liability was the underlying principle in the *Hedley Byrne* case.[102]

> "An assumption of responsibility by a person rendering professional or quasi professional services, coupled with reliance by the person for whom the services were rendered, could give rise to tortuous duty of care irrespective of whether there was a contractual relationship between the parties."[103]

This concept is however very controversial and has undergone a fair amount of criticism.[104] *White v Jones*[105] mediated the situation to a certain extend by stating that the ground on which the criticism is based is errorous, as voluntary assumption of responsibility does not refer to the defendant having assumed **legal responsibility**, but rather **responsibility for the task**.[106] The reason why the courts have had difficulty with

---

98 *Permanent Building Society (in liq) v Wheeler*, (1994) 11 WAR 187, 287-288.
99 (n 47) 13.
100 1964 AC 465.
101 1995 2 AC 145.
102 (n 100) AC 465.
103 (n 47) 8.
104 Some examples of cases which criticise the voluntary assumption of responsibility principle include *Smith v Bush* 1990 1 AC 831; 862 and *Caparo Industries v Dickman* 1990 2 AC 605 at 628.
105 1995 2 AC 207.
106 (n 47) 9.

this concept was because of the fact that they confuse that which the defendant assumed responsibility for:[107]

> "…but the assumption of responsibility referred to is the defendants' assumption of responsibility for the task, not the assumption of legal liability…If the responsibility for the task is assumed by the defendant he thereby creates a special relationship between himself and the plaintiff in relation to which the law (not the defendant) attaches a duty to carry out carefully the task so assumed." [108]

It is not foreseen that South African courts will have any problems adopting this principle into our law, as it is common practice amongst South African courts to, in cases where no guidance can be found in our law, look to English law and English precedents on the point in issue, and draw from their experience. It is put forth that it is only a matter of time before we will see the first court case in this regard in South Africa.

7.8 Conclusion

From the above discussion it follows that the common law duty of care and skill may just as successfully be demanded and enforced in cyberspace as it has been in the physical world. The information age has not changed the nature of this duty, only its application, as a clear increase in demand for this duty, and austerity with which it is enforced may be observed. This trend should be a growing concern for anyone contemplating taking up the office of director.

Following the examples of English law, it is clear that the duty of care and skill will form the legal ground on which a director may be held personally liable for failed information security. Even more distressing is the fact that the emerging principle of voluntary assumption of responsibility is going to play a significant and increasingly important role in the years to come. Not only will directors now have to be mindful of the fact that they

---

107 ibid.
108 ibid.

owe all stakeholders, in the physical world and in cyberspace, a duty of care and skill/due diligence, they will also have to realise that by accepting the office of director, they are assuming responsibility for all the tasks associated with this position.

It may therefor be concluded that the law has succeeded in finding a way to hold those people responsible for information security accountable.[109] Consequently, anyone contemplating taking up the office of director must first of all make an in-depth study of the rights, obligations and duties that he or she will owe, not only to the organisation, but also to all stakeholders involved. [110] Furthermore, specifically within the information security domain, it is expected of directors to gain assurance that reasonable steps have been taken to secure the organisation's information assets.[111] Therefor, any director wishing to escape liability for failed information security must ask himself/herself two questions: "do you **think** your information assets are secure?" or "do you **know** they are secure?" The answer to this question will determine not only the fate of the organisation, but also that of its directors.[112]

[109] See Annexure O for an assessment of the board's involvement in, commitment to, and knowledge of information security.
[110] (n 47) 9.
[111] See Annexure P for an information security toolbox that will aid the board in fulfilling its multitude of onerous responsibilities.
[112] For a summary of the board and management's responsibilities for information security governance see Annexure Q.