THE POTENTIAL LIABILITY OF DIRECTORS FOR CORPORATE CYBER BREACHES IN SOUTH AFRICA

by

CHRISTOPHER DAVID APPANAH

submitted in accordance with partial fulfilment of the requirements for the degree of

MASTER OF LAWS

in the subject:

Corporate Law

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. J. GELDENHUYS

DECLARATION

Name: Christopher David Appanah

Student number: 47594063

Degree: Master of Laws: Corporate Law

THE POTENTIAL LIABILITY OF DIRECTORS FOR CORPORATE CYBER BREACHES IN SOUTH AFRICA

I declare that the above dissertation is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that I submitted the thesis/dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.

_____ _____

SIGNATURE DATE

ABSTRACT

The advances in technology across the world have brought with it new ways of conducting business in a connected economy. South African companies are no exception. However, with this wave of digital connection there are also associated dangers and risks to companies, such as cyber-attacks. A data breach can cost a company a lot of money. The financial fallout may have a severe impact on the company bottom line, erode the share value and the company public profile may decline. All these impacts may lead to the closure of the company with the knock-on negative effect on employees and the economy. Directors are charged with the responsibility of sound management of the company. This research investigates whether, and if so how, directors may be held liable by the company for the damages caused by a corporate cyber breach on the basis that the directors breached their duties of care, skill and diligence owed to the company in terms of the Companies Act 71 of 2008. The ambit of 'diligence' expected from directors is investigated and it is considered whether the duty imposes an oversight and monitoring obligation on directors. The question of whether directors may rely on the business judgment rule to escape liability is answered. It is concluded that the business judgment rule is not applicable in instances where directors have positive obligations of oversight and monitoring. The dissertation also explores how the delictual liability of directors may be established within the context of corporate cyber breaches. Recommendations are put forward on manners in which directors may avoid liability.

Keywords/ terms

Business judgment rule; corporate cyber breaches; cyber-attack; data breaches in companies; delictual liability of directors; duties of directors; duty of care, skill and diligence; financial impact of cyber breaches; Information Technology/ IT governance; liability of directors.

DEDICATION

I dedicate this Dissertation to:-

My late mother, Jessica Appanah. You pushed me to always reach for the stars. You always taught me to persevere and keep going despite adversity. It was that perseverance that drove me to finish this research in the face of many challenges.

My partner, Anthony. Thank you for your unwavering love, support and encouragement whilst I embarked on this academic journey.

ACKNOWLEDGMENTS

I want to express my sincere thanks to my supervisor, Prof. Judith Geldenhuys, whose considered and detailed guidance, encouraging comments, patience and enthusiasm gave me the confidence to conduct my research and express my opinions with conviction. Thank you for always keeping me on track and making sure that I crafted a dissertation that I am very proud of.

I would like to express my gratitude to my father, Michael Appanah, my brother, Nicholas Appanah and my future sister-in-law, Sumeshnee Govender, for their support and encouragement during the course of my academic journey.

Although they will never see this, I want to give gratitude to my puppies who sat with me every night for hours at a time giving me a sense of comfort and serving as my non-judgmental sounding boards to clear my thoughts.

My gratitude also goes to my friends for their support and encouragement, especially Naaheed Raboobee, Aneska Narandas and Lekha Daya. Thank you for cheering me on and keeping me motivated.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 INTRODUCTION

The advances in digital technology have created the perfect storm for cyber risks to emerge and threaten the stability of companies across the world and the vastly greater connected economic environment that companies operate within.[1] Klein AJ, in *Fourie v Van der Spuy and De Jongh Inc*[2] remarked that '[t]he rate at which cybercrime occurs makes the internet a very unsafe working area'.[3]

Cyber criminals leverage advancing technology to engage in complex criminal cyber activity to which companies may be vulnerable.[4] According to the Cost of Data Breach Report 2020 published by the Ponemon Institute, the cost of a data breach for a company in South Africa is USD 2.14 million.[5] A company in which a cyber breach occurs may have to fork out millions of rand in order to investigate and mitigate the possible effects of the breach.[6] The possible drop in share value and the loss of business would, no doubt, hit the bottom line of the company and may result in the shutdown of the company, which has far reaching economic consequences.[7]

1.2 PROBLEM STATEMENT

The increased frequency of corporate cyber breaches in South Africa and globally is the catalyst for this research.[8] The devastating financial impact a corporate cyber breach could potentially have on a company raises the question of whether the directors of the company can be held liable for the consequential financial losses. In this research, the potential liability of directors for a corporate cyber breach is explored within the context of directors' duties of care, skill and diligence. This duty is owed by

---

1 The potential devastating impact of a corporate cyber breach on a company is discussed in ch 2. See also Chitimira and Ncube 2021 PER / PELJ 2. At 3, the authors submit the that '[w]hile the increased reliance on the Internet offers many benefits to both human beings and banking institutions, it also provides new opportunities for unscrupulous persons to exploit both the common law and statutory regulatory gaps and commit cyber crimes'.

2 2020 (1) SA 560 (GP).

3 Paragraph 25.

4 Chitimira and Ncube 2021(24) PER/ PELJ 4.

5 IBM Corporation, 'Cost of a Data Breach Report 2020' 23. Available at www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use 9 March 2021).

6 IBM Corporation, 'Cost of a Data Breach Report 2020', 23. Available at www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use 9 March 2021).

7 This is discussed under 2.4.

8 See ch 2 in this regard.

a director to the company in terms of section 76(3)(c) of the Companies Act 71 of 2008 (the Act).[9] The devastation that corporate cyber breaches cause to companies cannot be underestimated given that there are legal and economic effects on a company.[10] It is therefore important for directors to understand their potential liability for losses suffered by a company as a result of a corporate cyber breach.[11] This research examines the inclusion 'diligence' in section 76(3)(c) of the Act, and the relevance of the duty with respect to corporate cyber breaches and the prevention thereof by directors.[12] The business judgment rule is analysed[13] with particular focus on whether directors can rely on this rule to escape liability if it is found that they have failed to discharge their duties of care, skill and diligence.[14] The approach taken in the United States of America (the USA) is outlined,[15] and a comparison is drawn between the USA's regulating principles and South Africa's.[16] As the USA has seen litigation on corporate cyber breaches and directors' liability therefore, a discussion on the approach taken by the courts in the USA is undertaken with the intention of gauging how the South Africa courts may deal with the issue.[17]

1.3 THE OBJECTIVE AND PURPOSE OF THE RESEARCH

The purpose of this research is firstly, to convey an understanding of the importance of corporate cyber breaches as a potential liability risk for directors. Further, the research aims to establish whether, and if so, on what basis, directors can be held liable to the company for damages that result from a corporate cyber breach on the basis that they have failed to discharge their duties of care, skill and diligence in terms of the Act. Thirdly, the research aims to postulate how delictual liability may be founded in terms of section 77(2)(b)(i) of the Act and to answer the question of whether liability may be avoided by the directors by relying on the business judgment rule. Lastly, this

9 Section 76(3)(c) of the Act. Directors' duties of care, skill and diligence is discussed in ch 3.
10 This is discussed in 2.4.
11 This is especially relevant given that the Act in terms of s 66(1) which states that '[t]he business and affairs of a company must be managed by or under the direction of its board, which has the authority to exercise all of the powers and perform any of the functions of the company, except to the extent that this Act or the company's Memorandum of Incorporation provides otherwise'. Section 76(3)(c) of the Act is the control built into the Act to ensure that the directors manage the affairs of the company with the necessary care, skill and diligence.
12 See the discussions under 3.3.2 and 4.5.3.
13 This is discussed in 3.4.
14 This is discussed in 3.4 and 5.3.3.
15 See the discussion in ch 4.
16 This is discussed under 4.6.
17 This is examined in ch 4.

research aims to provide possible recommendations to directors on how they may mitigate potential liability to the company for damages caused as a result of a corporate cyber breach.

1.4 RESEARCH METHODOLOGY

This research is conducted by way of reviewing the applicable jurisprudence as well as research articles so far as it relates to data protection and cyber security. The company law jurisprudence of South Africa and the USA is examined with respect to the directors' duties of care, skill and diligence as well as the business judgment rule. Litigated matters within the USA are analysed insofar as they relate to the directors' duties and their liability for corporate cyber breaches. The conclusion provides recommendations supported by the facts, precedents and legislation reviewed during this research.

1.5 CHAPTER OVERVIEW

Chapter 1 is the introduction, which gives an overview of the contents of the research reports, the research aims, the research methodology and the chapter synopsis.

Chapter 2 defines the concept 'corporate cyber breaches' for the purposes of this research.[18] The distinction between 'cyber breaches' and 'data breaches' is highlighted.[19] The potential negative impacts on a company as a result of a corporate cyber breach is outlined briefly.[20] Legal and regulatory aspects insofar as these relate to corporate cyber breaches are highlighted.[21] This chapter sets the contextual background against which this research is conducted. It is explained that directors have a statutory management duty towards the company and their liability to the company is established on the basis of whether they have breached their duties of care, skill and diligence in terms of the Act.[22]

In Chapter 3 the duties of care, skill and diligence is examined. A discussion of the codified duty of care, skill and diligence in terms of section 76(3)(c) of the Act highlights that a subjective and objective assessment is required to determine if the directors

18 See the discussion under 2.2 and 2.3.
19 This is discussed under 2.3.
20 Discussed in 2.4 and 2.7.
21 See the discussion under 2.7.
22 See the discussions under 2.7 and 2.8.

have discharged their duties.[23] It is established that diligence means that directors have a legislated oversight and monitoring duty.[24] The business judgment rule is examined and it is indicated that the rule provides a safe harbour for directors from hindsight reviews of their business decisions.[25] Interestingly, it is established that the business judgment does not apply to situations where directors have not discharged their duties of oversight and monitoring.[26]

Chapter 4 undertakes a review of the USA position with respect to directors' duty of care[27] and the business judgment rule.[28] It is highlighted that the duty of care in USA company law jurisprudence includes the duty of oversight and monitoring of the company, which is comparable to the duty of diligence required by the Act in South Africa.[29] An analysis of case law in the USA reveals that a breach of oversight is easily ascertainable where there is a positive duty ('positive obligations') placed on the directors and they fail to discharge that duty.[30] The analysis of the application of Delaware corporate law on the point of 'positive obligations' forms the foundation of the author's view that the increased risk of corporate cyber breaches, legislation related to IT risks and the King IV Report may be relied on to found the 'positive obligations' within the context of the duty of diligence in South Africa.[31]

In Chapter 5, the basis of liability of directors for a breach of the duty of care, skill and diligence within the context of corporate cyber breaches is examined by analysing section 77(2)(b)(i) of the Act. Whether a breach of the directors' duty of care, skill and diligence occurred is determined by applying the principles of delict.[32] Therefore, the five elements of a delict are examined within the context of a corporate cyber breach and the directors, duties of care, skill and diligence.[33] Notably, with respect to negligence an objective and subjective assessment of the directors' conduct must be undertaken.[34] The objective leg requires that an assessment of the directors' conduct

---

23 This is discussed in 3.3.
24 See the discussion under 3.3.
25 This is discussed under 3.4.
26 See the discussion under 3.4.
27 This is discussed under 4.3.
28 See the discussion under 4.4.
29 See the discussion under 4.3.
30 This conclusion is reached under 4.5.3.
31 See the discussion under 4.7.
32 This is discussed in 5.2.
33 See the discussions under 5.3.
34 This aspect is discussed in 5.3.3.

be measured against the conduct of the reasonable person in the position of the director under the relevant circumstances, the subjective leg only becomes relevant in cases where the director in question has special skills or experience.[35] It is established that the attributes and conduct of the reasonable person is determined against the prevailing environmental conditions.[36] Consequently, within the context of this research it means that if a reasonable person would be aware of the corporate cyber issues, specifically the threat of corporate cyber breaches he or she ought to take the necessary and reasonable preventive steps.[37] It is established that certain 'positive obligations' establish a minimum standard of diligence (oversight and monitoring) applicable to directors with respect to corporate cyber issues.[38] The chapter further outlines that the 'positive obligations' with respect to oversight and monitoring duties of directors (the duty of diligence) do not fall within the ambit of a business decision and the directors cannot rely on the business judgment rule to escape liability where they have failed to discharge this duty.[39] It is, accordingly, established that directors may be held liable for corporate cyber breaches where they have failed in their duties of oversight and monitoring.[40]

Chapter 6 is the Conclusion, which provides an overview of the findings in the research report.[41] Recommendations are put forward as to what directors may do to mitigate liability.[42]

35 See the discussion under 5.3.3.
36 Concluded under 5.3.3 and 5.5.
37 See the discussion under 5.3.3. and 5.5.
38 This is discussed under 5.3.3.
39 See the discussion under 5.3.3.
40 This conclusion is reached under 5.5.
41 Discussed under 6.1, 6.2 and 6.3.
42 See the discussion under 6.4.

CHAPTER 2 CORPORATE CYBER BREACHES

2.1 INTRODUCTION

In this chapter, the concept 'corporate cyber breaches' is defined.[43] Within the context of this research, a 'corporate cyber breach' refers broadly to a 'cyber security breach' as well as a 'data breach'. These types of breaches are distinct from each other. This chapter explains the distinctive features of each type of breach.[44]

The potential negative impact of such breaches on a company is outlined.[45] The impetus for the adoption of sound legislative measures to curtail the potential negative effects is explained.[46] The potential negative effects of cyber breaches on South African companies are briefly set out.[47]

2.2 CYBER SECURITY BREACH

A cyber security breach occurs when a cybercriminal hacks into a company's system by finding a way around security controls, thus gaining unauthorised access to the computer system, software or digital information which is valuable to the company.[48] A cyber security breach is preceded by a cyber-attack which may manifest itself, among other things, as a virus, spyware, malware, phishing or denial of service attack.[49] A cyber security breach is then characterised by a successful cyber-attack which leads to the cybercriminal gaining unauthorised access to the company's computer system, software or digitally stored data.[50] Predominantly, a cyber security breach occurs first and may lead to a data breach. In some cases, a data breach can also occur without a breach in security, for example when a company negligently discloses information held on their systems.[51]

---

43 See the discussion under 2.2 and 2.3.
44 See the discussion under 2.2 and 2.3.
45 This is discussed under 2.7.
46 See the discussion under 2.6.
47 See the discussion under 2.7.
48 Norton 'What is a security breach'. Available at https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html (Date of use: 15 September 2020).
49 Gorecki 'A Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk' 11.
50 Gorecki 'A Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk' 11.
51 Norton 'What is a security breach'. Available at https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html (Date of use: 15 September 2020).

The Cybercrimes Act 19 of 2020 (the Cybercrimes Act) criminalises the unauthorised access of a computer program, data storage, system or data.[52] The Cybercrimes Act provides a definition of a cyber security breach which is worded widely to include 'alteration', 'modification', 'deletion', 'copying', 'moving data', 'use', 'instruction', and 'communication'.[53] All of these terms amount to access. If the access is unauthorised, then the person gaining unauthorised access to the computer system, software or digital information of the company would be guilty of an offence.[54]

2.3 DATA BREACH

A data breach is not synonymous with a cyber security breach and vice versa, these are distinct instances.[55] This means that not all cyber security breaches lead to a data breach and not all data breaches arise from a cyber security breach. In the main, data breaches are usually preceded by a cyber security breach.[56] A general definition of a 'data breach' means the 'unauthorised disclosure'[57] of confidential information. A data breach is an unlawful and intentional interception of data.[58]

Section 3(4) of the Cybercrimes Act defines the interception of data as follows:

> For purposes of this section 'interception of data' means the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool contemplated in section 4(2) or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data, and includes the—
>
> a) examination or inspection of the contents of the data; and

---

52 Chapter 2, Part 1 of the Cybercrimes Act relates to specific cybercrimes. See ss 2(2)(a)-(b), 3(1), 4(1), 5(1), 6(1) and 7(1)–(3) of the Cybercrimes Act.

53 Section 2(2)(a)-(c) of the Cybercrimes Act.

54 Section 2(1) and 2(2) of the Cybercrimes Act reads:
'2(1) Any person who unlawfully and intentionally performs an act in respect of—
(a) a computer system; or
(b) a computer data storage medium,
which places the person who performed the act or any other person in a position to commit an offence contemplated in subsection (2), section 3(1), 5(1) or 6(1), is guilty of an offence.
(2)(a) Any person who unlawfully and intentionally accesses a computer system or a computer data storage medium, is guilty of an offence'.

55 Gorecki 'Cyber Breach Response that Actually Works: Organizational Approach to Managing Residual Risk' 11.

56 Fowler 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 2.

57 Gorecki 'A Cyber Breach Response that Actually Works: Organizational Approach to Managing Residual Risk' 11.

58 Section 3(1) of the Cybercrimes Act.

b) diversion of the data or any part thereof from its intended destination to any other destination.

Data breaches commonly occur as a result of a successful cyber-attack, whether intentional or opportunistic in nature.[59] Data breaches also occur in cases where employees either accidentally or negligently cause confidential information to be disclosed. This can happen if an employee is entrusted with data and the employee is negligent in the manner that they store or transport the data.[60] This is what occurred when Experian Information Solutions Incorporated (Experian) suffered a data breach that exposed the personal information of approximately 24 million South Africans and an estimated 800 000 businesses due to a fraudulent data inquiry where employee negligence led to the disclosure of the data.[61] It is submitted that a data breach can be both intentional and negligent depending on the surrounding circumstances that led to the breach.

Notably, where a data breach leads to the compromise of more than one million records, the breach is termed a mega breach.[62] The global average cost of a mega breach is USD 392 million, which represents a hundredfold increase in the average cost of a data breach.[63]

2.4 FINANCIAL IMPACT OF A DATA BREACH

The costs associated with a data breach can be categorised as direct, indirect and systemic costs.[64]

Direct costs refer to the costs incurred by a company immediately after a data breach occurs.[65] These include costs to contain and investigate as well as regulatory and legal costs.[66] According to the Cost of Data Breach Report 2020, the global average direct

59 Fowler, 'Data Breach Preparation and Response: Breaches Are Certain, Impact is Not' 6.
60 Fowler, 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 6.
61 Hosken, 'Data from huge Experian breach found on the internet'. Available at https://www.timeslive.co.za/sunday-times/news/2020-09-13-data-from-huge-experian-breach-found-on-the-internet/ (Date of use: 14 September 2020).
62 IBM Corporation, 'Cost of a Data Breach Report 2020' 66. Available at www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use: 9 March 2021).
63 IBM Corporation, 'Cost of a Data Breach Report 2020' 67. Available at www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use 9 March 2021).
64 Fowler, 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 20.
65 Fowler, 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 20.
66 Fowler, 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 20.

cost of a data breach per record is USD 146.[67] This translates to more than USD 3 billion for the Experian data breach.

Indirect costs refer, among other things, to the costs on the brand, share value, resources, time and effort spent by the company after a data breach.[68] In 2016, Yahoo reported a data breach of 500 million customer accounts two years after they became aware, thus causing the company a loss in share value of USD 1.5 billion.[69]

Systemic costs refer to incidental costs associated with the data breach.[70] For example, this includes the costs that may be incurred where stolen customer data was used for fraudulent transactions which must be reversed.[71] Such reversal charges are payable by the company. In 2013, USA retailer Target suffered a data breach where over 100 million customer records were stolen.[72] Target settled USD 100 million in systemic costs to financial institutions who refunded customers for funds lost as a result of the data breach.[73]

2.5 RISK MANAGEMENT

'Risk management' within the context of corporate cyber breaches refers to the identification, assessment and monitoring of cyber risks so that such risks are managed within the risk appetite of the company.[74] The aim is to prevent cyber-attacks, or alternatively to mitigate the effect of a corporate cyber breach on a company.[75]

---

67 IBM Corporation, 'Cost of a Data Breach Report 2020' 17. Available at www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use: 9 March 2021).

68 Fowler, 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 22.

69 Whitler and Farris 2017 JAR 3–4.

70 Fowler, 'Data Breach Preparation and Response: Breaches are Certain, Impact is Not' 23.

71 See Chitimira and Ncube 2021 PER / PELJ 4. The authors explain that this has happened in South Africa when 'a criminal syndicate reportedly created and employed a malware known as 'Dexter' to attack a number of South African retailers and stole millions of Rands. This malware intercepted the payment details of ignorant customers from the point-of-sale terminals of retailers, created fraudulent duplicate bank cards, and stole money from the retailers and from their customers'.

72 Whitler and Farris 2017 JAR 4.

73 Whitler and Farris 2017 JAR 5.

74 Gorecki, 'A Cyber Breach Response that Actually Works: Organizational Approach to Managing Residual Risk' 13.

75 Gorecki, 'A Cyber Breach Response that Actually Works: Organizational Approach to Managing Residual Risk' 13.

Cyber risks are constantly evolving. As a result, companies are not completely immune to corporate cyber breaches.[76] This means that companies must rather ensure that they are prepared when a corporate cyber breach occurs.[77] Cyber risk management is not simply a tick box exercise that can be completed once, it is a dynamic process with many iterations and should evolve much like the complex cyber risk environment.[78]

2.6 THE IMPETUS FOR ADOPTING SOUND REGULATORY MEASURES

The World Economic Forum's Global Risks Report 2021 identifies cyber security failure as the fourth critical threat to the world.[79] The current digital age has brought about an increased corporate digital footprint in general.[80] Vast amounts of data are held by large corporations.[81] These data stores are tempting to cyber criminals and, as a result, this data requires protection, much like physical assets.[82] In the recent case of *S v Msomi*[83] Smith J held:

> The overwhelming demand for secure internet banking and shopping means that financial institutions are becoming increasingly dependent on secure cyber transactions in order to conduct their business effectively. The public sector, and for that matter private individuals and companies, is also equally reliant on access

76 Cybok, 'The Cyber Security Body of Knowledge' 25. Available at https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf (Date of use: 10 March 2021).

77 Cybok, 'The Cyber Security Body of Knowledge' 25. Available at https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf (Date of use: 10 March 2021).

78 Cybok, 'The Cyber Security Body of Knowledge' 46. Available at https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf (Date of use: 10 March 2021).

79 World Economic Forum, 'The Global Risks Report 2021' 11. Available at http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (Date of use: 10 March 2021).

80 Gorecki, 'A Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk' 1. See also Hamadziripi and Chitimira 2021 PER / PELJ 2 where the authors state that '[t]he most influential means of change in contemporary business society is technology because it is convenient to businesses and their clients' and further that 'technology has ceased to be a mere business enabler but is now a source of a company's future opportunities'.

81 Gorecki, 'A Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk' 1. See also Hamadziripi and Chitimira 2021 PER / PELJ 11, the authors emphasise the vastness of the data stored by companies by stating that '[t]he volume and diversity of data available to companies in South Africa cannot be analysed manually, and in most cases it exceeds the capacity of conventional databases'.

82 Gorecki, 'A Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk' 1. See also Cassim 2011 CILSA 123, the author submits that '[c]yber crime is thriving on the African continent. The increase in broadband access has resulted in an increase in internet users. Thus, Africa has become a 'safe haven' for online fraudsters. African countries are pre-occupied with pressing issues such as poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes, such as murder, rape, and theft. As a result, the fight against cyber-crime is lagging behind'. It is interesting that Cassim made this statement in 2011, it is, therefore, submitted that the threat of cybercrime within the South African context has increased substantially since 2011.

83 2020 (1) SACR 197 (ECG).

> to secure internet banking. The ability of cyber 'hackers' to infiltrate these electronic systems for their own selfish purposes consequently has far-reaching and deleterious consequences for the economy, both domestically and globally.[84]

This statement by Smith J reflects an enlightened judicial system that is aware of the cyber risks associated with the connected economy that companies operate within. It is submitted that courts are therefore not blind to the potential consequences that a corporate cyber breach may potentially have on a company.

Companies across the world have experienced tremendous corporate cyber breaches. In the United Kingdom, a cyber-attack led to a loss of GBP 92 million to the NHS.[85] In 2016, Yahoo experienced a data breach where three billion users' account information was stolen by cyber attackers, costing the company value to fall by approximately USD 350 million.[86] In South Africa during 2020, Experian suffered a data breach which resulted in the exposure of 24 million South African's user information.[87]

There has been a marked increase in the rate of cyber security breaches in South Africa since the beginning of the Covid-19 pandemic.[88] Therefore, the risk of a company being subjected to such an attack is higher, necessitating the need for companies to implement an appropriate plan to deter or to prevent cyber breaches, and to mitigate the negative effects of a cyber-related incident.

2.7 THE POTENTIAL NEGATIVE EFFECTS OF CYBER BREACHES IN THE SOUTH AFRICAN CONTEXT

Within the South African context, businesses are faced with an economy that is unstable due to the COVID-19 pandemic and related government induced lockdowns,

---

84 Paragraph 34.

85 Acronis, 'The NHS Cyber Attack: How and Why It Happened, and Who Did It'. Available at www.acronis.com/en-us/articles/nhs-cyber-attack/ (Date of use: 10 March 2021).

86 Swinhoe, 'The 18 Biggest Data Breaches of the 21st Century'. Available at www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (Date of use: 10 March 2021).

87 Hosken, 'Data from huge Experian breach found on the internet'. Available at https://www.timeslive.co.za/sunday-times/news/2020-09-13-data-from-huge-experian-breach-found-on-the-internet/ (Date of use 14 September 2020). Also see fn 428 for further examples of corporate cyber breaches which have occurred in South Africa.

88 Mimecast, 'The State of Email Security 2020'. Available at https://www.mimecast.com/globalassets/cyber-resilience-content/the_state_of_email_security_report_2020.pdf (Date of use: 16 September 2020).

poor electrical infrastructure and socio-political challenges.[89] Given these challenges, along with the potential costs of a data breach, the potential for business closures as a result of data breaches is great.

According to the Cost of a Data Breach Report 2020 compiled by the Ponemon Institute, published by the IBM Corporation, the average cost of a data breach in South Africa is USD 2.14 million.[90] This figure illustrates the immense cost a data breach can have on the bottom-line of a business, which may have significant impact on the continuity of the business itself.[91] The direct cost of a data breach can severely impact a South African company's bottom-line, including impacts on reputation, company share value, and consumer trust and employee performance.[92] This may have significant impact on the continuity of the business itself.[93]

The Protection of Personal Information Act 4 of 2013 ('the POPI Act'), under section 19, places an obligation on companies that process personal information to secure the 'integrity and confidentiality of personal information' in their possession.[94] The company must take 'appropriate, reasonable technical and organisational measures' to prevent loss of any nature whatsoever as well as unlawful access or processing of personal data.[95] The POPI Act enumerates the measures that a company can take to discharge its duty in terms of section 19(1). The measures include identifying all reasonably foreseeable internal and external risks, implementing and maintaining necessary safeguards against those risks, assessing the effectiveness of the risk safeguards regularly and ensuring that the risk safeguards are continually updated to stay ahead of emerging risk trends not previously catered for.[96]

Section 22 of the POPI Act places an obligation on companies to notify parties should they suffer a data breach where sensitive information may have been accessed or stolen by an unauthorised individual. Section 73 of the POPI Act deems non-

89 SEDA, 'SMME Quarterly Update 3rd Quarter 2020' 5. Available at http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%20Sector%20Report%20Q3%202020.pdf (Date of use: 24 March 2021).
90 IBM Corporation, 'Cost of a Data Breach Report 2020' 23. Available at www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use 9 March 2021).
91 Fowler, 'Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not' 20.
92 Fowler, 'Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not' 20.
93 Fowler, 'Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not' 20.
94 Section 19(1) of the POPI Act.
95 Section 19(1)(a) and (b) of the POPI Act.
96 Section 19(2)(a)–(d) of the POPI Act.

compliance to the reporting requirement under section 22 as an interference with the protection of personal information.[97] In terms of section 99 of the POPI Act, an organisation may face civil litigation for damages instituted by the Information Regulator due to a breach of section 73.[98] The company may be held strictly liable with limited defences available to it.[99] The POPI Act speaks to administrative fines that a company may incur as a result of committing an offence under the act. The administrative fine is capped at R10 million.[100]

Section 54(1) of the Cybercrimes Act places an obligation on an electronic services provider and financial institutions to report corporate cyber breaches to the South African Police Service (SAPS) within 72 hours.[101] This obligation runs parallel to section 22 of the POPI Act, and the applicable companies must report a corporate cyber breach to both the Information Regulator and SAPS within distinct timeframes.[102] A breach of section 54(1) of the Cybercrimes Act may attract a fine.[103]

The author submits that the legislated responsibility of a company to protect personal data that it processes, along with the notification obligations and possible administrative fines, bolsters the negative effect that a corporate cyber breach can have on a company, its bottom-line and reputation. The legislature has made it

---

97 Section 73(b) of the POPI Act.

98 Section 99(1) of the POPI Act.

99 Section 99(2) of the POPI Act states:

'In the event of a breach the responsible party may raise any of the following defences against an action for damages:

(a) Vis major;
(b) consent of the plaintiff;
(c) fault on the part of the plaintiff;
(d) compliance was not reasonably practicable in the circumstances of the particular case; or
(e) the Regulator has granted an exemption in terms of section 37'.

100 Section 109(2) of the POPI Act.

101 Section 54(1) of the Cybercrimes Act states as follows:

'An electronic communications service provider or financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must—

(a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and

(b) preserve any information which may be of assistance to the South African Police Service in investigating the offence.'.

102 In terms of s 22 of the POPI Act the timeframe is 'as soon as reasonably possible' and s 54(1) of the Cybercrimes Act the timeframe is 'not later than 72 hours'.

103 Section 54(3) of the Cybercrimes Act reads:

'An electronic communications service provider or financial institution that fails to comply with subsection (1), is guilty of an offence and is liable on conviction to a fine not exceeding R50 000'.

abundantly clear that these obligations must be complied with. There is no doubt that ensuring compliance remains the duty of the board of directors.[104]

Considering the liquidity of a company, if a company is not able to pay its debts, even though its assets may exceed its liabilities, then such company is commercially insolvent.[105] The financial impact of a data breach could have disastrous effects on the commercial solvency of a company, and could result in the company being wound up in terms of the Companies Act 61 of 1973 (the 1973 Act).[106] Additionally, the company may be prohibited from trading in terms of section 22 of the Companies Act 71 of 2008 (the Companies Act).[107] Section 22 empowers the Companies and Intellectual Property Commission ('the CIPC') to serve a notice on a company to show good cause why it should be allowed to continue business where the CIPC, on reasonable grounds, believes the company is trading in contravention of section 22(1) of the Companies Act, or is commercially insolvent.

Section 22 must be read with section 77(3)(b) of the Companies Act, which provides that a director may be held liable to the company for any loss, damages or costs incurred by the company as a direct or indirect consequence of the director either (a) agreeing to conducting the business in a manner prohibited in terms of section 22, or (b) playing a part in a plan to conduct the business in a manner that was aimed to

---

104 Section 66(1) of the Act states that '[t]he business and affairs of a company must be managed by or under the direction of its board, which has the authority to exercise all of the powers and perform any of the functions of the company, except to the extent that this Act or the company's Memorandum of Incorporation provides otherwise'. Accordingly, the duty to ensure that the company complies with the POPI Act rests with the directors of the company. See also Delport, *Henochsberg on the Companies Act 71 of 2008* 250(2).

105 Swart and Lombard 2015 THRHR 357. In *Boschpoort Ondernemings (Pty) Ltd v ABSA Bank Ltd* 2014 (2) SA 518 (SCA) the court explained that South African jurisprudence recognised factual and commercial insolvency. A company is factually insolvent if the company's liabilities exceed its assets, however the company may still be able to pay its debts. A company is commercially insolvent if it is unable to pay its debts, even though its assets may exceed its liabilities. The court then confirmed that a company's commercial insolvency is the accepted standard in South Africa for liquidation of a company. At para 23, the court specifically indicated that factual solvency is not a determining factor on whether a company is liquidated or not.

106 Section 344 of the 1973 Act provides that a company may be wound up if it is deemed unable to pay its debts in terms of s 345 of the 1973 Act. In *Boschpoort Ondernemings (Pty) Ltd v ABSA Bank Ltd* 2014 (2) SA 518 (SCA) para 10, the court stated that where a company is unable to pay its debts as provided in s 345 of the 1973 Act, then such company may be wound up in terms of section 344. See Cassim and others, *Contemporary Company Law* 918–919. See Swart and Lombard 2015 THRHR 357.

107 Section 22(1) of the Act prohibits companies from conducting business recklessly, or with intent to defraud, or with gross negligence. An additional layer was added by the legislature in the form of prohibiting companies from insolvent trading. See Cassim and others, *Contemporary Company Law* 592.

defraud a company stakeholder or for another fraudulent purpose. Interestingly, this section speaks to the company holding the offending director liable for its heads of damages, which substantially increases the risk for a director.[108]

Given the identified challenges faced in the country, along with the potential costs of a data breach, arguably the possibility of a business closing as a result of a data breach is great. It is further submitted that the likelihood of the company being held liable by a third-party as a result of a data breach is high. Considering the legislated management duties of directors to the company, the question then arises as to whether the directors may be held liable for damages suffered by the company as result of a corporate cyber breach?[109] To answer this question, consideration must be given to directors' duties of care, skill and diligence and whether the happening of a corporate cyber breach means that the directors may be held liable to the company.[110]

2.8 CONCLUDING REMARKS

This chapter has outlined the meaning of 'corporate cyber breaches' within the context of this research to show that it includes both 'cyber security breaches' and 'data breaches'.[111] It is apparent that data-related corporate cyber breaches pose the greatest threat to the continued existence of a company. The extraordinarily high financial cost and resultant reputational impact that can potentially ensue in the event of a corporate cyber breach provide the impetus for the regulation of cyber breaches.[112]

Preventative controls and mitigation plans are essential if a company is to weather the potential storm of a corporate cyber breach. Although these plans may not necessarily guarantee a company's survival, these provide some measure of mitigation against this major risk.[113]

South African corporate law dictates that where a company becomes commercially insolvent the company can be liquidated and prohibited from trading.[114] Given the

---

108 Phungula 2016 SA Merc Law J 248. See also *Rabinowitz v Van Graan and Others* 2013 (5) SA 315 (GSJ) paras 22–23.
109 See fn 104 regarding the management duties of directors in terms of the Act.
110 This is discussed in ch 3.
111 See the discussions under 2.2 and 2.3.
112 As discussed under 2.4.
113 See the discussion under 2.5.
114 See the discussion under 2.7.

financial impact of a corporate cyber breach, a creditor may easily approach a court and make a case for liquidation, thereby causing the dissolution of the company, often on less than favourable terms for all its stakeholders.[115]

The management of the company is legislated as the responsibility of the directors therefore the liability for the devastation caused to a company as a result of a corporate cyber breach may be claimable in turn from the directors of the company on the basis that the directors have breached their duties of care, skill and diligence in terms of the Act.[116]

In the following chapter an analysis of the legal and regulatory landscape in South Africa is undertaken, including directors' duties of care, skill and diligence,[117] the business judgment rule[118] and the technological governance and security requirements of the Institute of Directors of South Africa's *King Report on Corporate Governance, 2016* (the King IV). Given the personal liability that may befall a director,[119] this analysis outlines the legal framework that governs directors' duties with respect to implementing adequate measures to mitigate the effects of a corporate cyber breach on an organisation.

115 Discussed under 2.4.
116 See discussion in 2.7.
117 Section 76(3)(c) of the Companies Act.
118 Section 76(4)(a) of the Companies Act.
119 Discussed under 2.7.

CHAPTER 3 THE DUTY OF CARE, SKILL AND DILIGENCE, THE BUSINESS JUDGMENT RULE AND THE KING IV

3.1 INTRODUCTION

In this chapter, the common law directors' duty of care and skill is discussed to provide the contextual basis of the partial codification of these duties into the Act.[120] The directors' duty of care, skill and diligence as it is now known in terms of the Act, is examined.[121] Notably, it is established that the duty of care, skill and diligence is owed by all directors as well as prescribed officers.[122] An examination of the introduction of 'diligence' is undertaken, with a finding that 'diligence' means that directors have a legislated oversight and monitoring responsibility.[123] The blended objective–subjective test is established by the Act, against which the duties of care, skill and diligence is considered.[124] A discussion of the business judgment rule reveals that a director's decision, although it may appear to be unreasonable may still meet the rationality requirement of the business judgment rule, therefore, affording the director a safe harbour from judicial review of their decision.[125] Notably, it is established that the business judgment rule does not apply where the directors fail to discharge their oversight and monitoring duties.[126] The recommendations enumerated in the King IV to Information Technology (IT) governance are discussed, and the impact of the King IV in the assessment of whether a director has complied with the duty of care, skill and diligence is considered.[127]

3.2 THE COMMON LAW DIRECTORS' DUTY OF CARE AND SKILL

The potential loss to a company as a result of a corporate cyber breach may prompt the company to pursue a claim for damages against the directors.[128] The liability to the company may be founded in delict if the directors' conduct meets the requirements of

120 See the discussion under 3.1.
121 See the discussion under 3.3.
122 This is discussed under 3.3.1.
123 See the discussion under 3.3.2.
124 This is discussed under 3.3.2.
125 Discussed under 3.4.
126 Discussed under 3.4.
127 This is discussed under 3.5.
128 See the discussion under 2.7.

a delict.[129] This assessment involves determining whether the directors have breached their duty of care, skill and diligence.[130]

Prior to the partial codification of the duties owed by directors into the Act,[131] directors' duties—particularly the directors' duty of care and skill as it was then known—were guided by common law.[132] The Act did not exclude the common law to the extent that it does not conflict with the Act.[133] The body of common law with respect to directors' duties of care and skill provide context on the principles that have been carried through to the Act, thus providing a holistic view into what the duty entails.

The South African common law relating to the duty of care and skill was largely drawn from English jurisprudence.[134] The English common law appeared to have given directors the 'freedom to manage companies incompetently',[135] requiring the presence of gross negligence before a director could be held liable for decisions that negatively impacted the company.[136] In *Re Denham & Co*[137] a director was found to be negligent for not performing his duties for a period of four years. However, the court did not find that he had been in breach of his duty of care. This bolsters the view that conduct which exceeded ordinary negligence was required for liability to ensue.[138] English courts required very little of directors in terms of the standard of care and skill exercised.[139] The rationale for the tolerant view that was taken by English courts was that the shareholders appointed the directors, and that they should be accountable for their decisions.[140]

---

129 Mupangavanhu 2017 SteII LR 158. The author distinguishes between the directors' fiduciary duties and duties of care, skill and diligence. See also s 77(2)(b)(i) of the Act.

130 Mupangavanhu 2017 SteII LR 158.

131 See the discussion in 3.3.

132 Delport, Henochsberg on the Companies Act 71 of 2008 295. See also Cassim and others, Contemporary Company Law 554.

133 Delport, Henochsberg on the Companies Act 71 of 2008 296.

134 Bekink 2008 SA Merc LJ 97. See also Bouwman 2009 SA Merc LJ 510 and Havenga 2000 SA Merc LJ 25. See Cassim and others, *Contemporary Company Law* 557.

135 Bekink 2008 SA Merc LJ 97.

136 Bekink 2008 SA Merc LJ 97.

137 (1884) LR 25 Ch D 752.

138 Bouwman 2009 SA Merc LJ 512. See also *In Re Denham & Co* (1884) LR 25 Ch D 764–768.

139 Bouwman 2009 SA Merc LJ 511.

140 Bouwman 2009 SA Merc LJ 511. Bouwman explains a further rationale, i.e that directors of the time were appointed for their reputation and not for their business acumen. See also *Turquand v Marshall* (1868-69) LR 4 Ch App 376. The court held (at 386) that 'however ridiculous and absurd their conduct might seem, it was the misfortune of the company that they chose such unwise directors; but as long as they kept within the powers of their deed, the Court could not interfere with the discretion exercised by them.'

In *Re Brazilian Rubber Plantations and Estates Ltd*[141] the directors received a fraudulent report which they relied on to purchase a plantation. The issues revolved around the fact that the directors were aware of the misrepresentations and inconsistencies surrounding the transaction.[142] However, the directors had done nothing further to address the known red flags.[143] Instead, the directors entered into the contract to the company's detriment and the company was subsequently wound up.[144] The liquidator alleged that the directors had been grossly negligent in concluding the contract despite their knowledge of the fraudulent elements.[145] Neville J, in finding that the directors had not been grossly negligent, formulated an enquiry to determine gross negligence by assessing the degree of the duty that the director was alleged to have neglected.[146] In his assessment, the judge took the view that directors' duties required the director to act with the level of care reasonably expected from him given his experience and knowledge.[147] The court took a skewed view on the degree of skill required by a director by stating that a director who was highly knowledgeable or experienced on the subject under contention 'must give the company the advantage of his knowledge'.[148] At the same time, the court indicated that an inexperienced or unknowledgeable director may not attract liability for their uninformed decisions which may lead to mistakes occurring.[149] This imbalanced approach, the author submits, appears to place higher risk on a seasoned director as compared to an inexperienced director with respect to a decision made by both on the same subject under consideration within our present corporate contextual environment.[150]

---

141 [1911] Ch 425.
142 [1911] Ch 425 427–428.
143 [1911] Ch 425, 428.
144 [1911] Ch 425, 429.
145 [1911] Ch 425, 429.
146 [1911] Ch 425 (437) the court held as follows: 'In truth, one cannot say whether a man has been guilty of negligence, gross or otherwise, unless one can determine what is the extent of the duty which he is alleged to have neglected.'
147 [1911] Ch 425, 437.
148 [1911] Ch 425, 437.
149 [1911] Ch 425, 437.
150 In Havenga 2000 SA Merc LJ 26, the author speaks to the contextual setting of the time when a lenient approach was taken by courts with respect to directors' duties. Notably, Havenga wrote: 'An alternative basis for the lenient approach was the assumption that directors were benevolent amateurs, lacking in any specialist or technical talent, who could not be expected to maintain a great involvement in company affairs, much less exercise the skills of a professional.' See also Farrar 2011 SAcLJ 749.

The *locus classicus* case of *Re Equitable Fire Insurance Co Ltd*[151] is considered to be the genesis of the common law director's duty of care.[152] The facts concerned fraud in the amount of GPB 1,2 million committed by the chairman of the company, for which the company liquidator wished to hold the directors liable for on the basis that they negligently failed to discover the fraud.[153] The court, per Romer J, put forward three propositions of law with respect to directors' duties of care.[154] First, Romer J explained that a director was required to apply the standard of care that an ordinary person may apply in a certain situation. However, the skill which the director applies is limited to their own experience and knowledge.[155] The challenge with this formulation, the author submits, is that a director's decision is measured against a bar set only as low as they are skilled, experienced and educated.[156]

Drawing on and endorsing the position taken by the English courts in *Re Equitable Fire Insurance Co Ltd*[157] and *Re Brazilian Rubber Plantations and Estates Ltd*,[158] in the South African *locus classicus* case, *Fisheries Development Corporation of SA Ltd v Jorgensen,*[159] Margo J expressed the following principles:

- A director should 'exercise the care which can reasonably be expected of a person with his knowledge and experience'.[160] A director is not required to have specialist knowledge or qualifications or experience in the business of the

151 [1925] Ch 407.

152 Bekink 2008 SA Merc LJ 98. See also Havenga 2000 SA Merc LJ 26 and Farrar 2011 SAcLJ 747.

153 [1925] Ch 407. See also McLennan 1996 SA Merc LJ 96 and Farrar 2011 SAcLJ 747.

154 [1925] Ch 427–429. See also Bekink 2008 SA Merc LJ 98, and McLennan 1996 SA Merc LJ 96–99. Farrar in 2011 SAcLJ 747 posits that there were four propositions by stating the following quote by Romer J as the first proposition: 'In discharging the duties of his position…a director must of course, act honestly; but he must also exercise some degree of both skill and diligence'.

155 [1925] Ch 407. At 428 it is held: 'A director need not exhibit in the performance of his duties a greater degree of skill than may reasonably be expected from a person of his knowledge and experience. A director of a life insurance company, for instance, does not guarantee that he has the skill of an actuary or a physician ... directors are not liable for mere errors of judgment'. See Cassim and others, *Contemporary Company Law*, 557. See also McLennan 1996 SA Merc LJ 96 and Farrar 2011 SAcLJ 748.

156 Interestingly in McLennan 1996 SA Merc LJ 96, McLennan opines that the proposition cannot be entirely subjective. It is argued that the use of the word 'reasonably' by Romer J should be interpreted in light of *Re Brazilian Rubber Plantations and Estates Ltd* [1911] Ch 425*,* where Neville J suggested (at 437) that the reasonableness required should be 'measured by the care an ordinary man might be expected to take in the same circumstances on his own behalf'. On this argument, a director who acts 'foolishly with impunity' may not escape liability for his failure to exercise his duty of care.

157 [1925] Ch 407.

158 [1911] Ch 425.

159 [1980] 4 All SA 525 (W).

160 [1980] 4 All SA 525 (W) 534.

company.[161] The standard of measurement is capped to the reasonable expectation of a person with the specific knowledge and experience of the director in question thus the enquiry suggested by Margo J is subjective in nature.[162] The court also expressed the view that directors are not to be held liable for 'mere errors of judgment'.[163]

- The court differentiated between executive and non-executive directors, saying that non-executive directors did not need to give the company affairs their continuous attention given the intermittent nature of their roles.[164] A director's duty of care is intrinsically linked to the nature of the business and the roles and duties assigned to or taken up by such director.[165]
- A director may delegate his duties to an official within the company in the absence of any suspicion that such official may not discharge such duties with conviction and honesty.[166] This means that a director can rely on the

---

161 Bouwman 2009 SA Merc LJ 511 and Bekink 2008 SA Merc LJ 100. See Cassim and others, *Contemporary Company Law*, 557; cf Du Plessis 2010 Acta Juridica 264. In Havenga 2000 SA Merc LJ 34, the author posits: 'No specific qualification is required to become a company director. Nonetheless, directors are expected to apply such skill as they do possess to the advantage of the company'.

162 Cassim and others, *Contemporary Company Law* 557. See also Havenga 2000 SA Merc LJ 34 where it is explained as follows: 'However, the standards according to which the degree of care and skill is to be measured are by no means clear. While it is to a certain extent possible to establish 'care' objectively, 'skill' varies from person to person.'

163 [1980] 4 All SA 525 (W) 534. Interestingly, the court did not allude to what may be considered as a mere lapse in judgment.

164 [1980] 4 All SA 525 (W) 534, Margo J held: 'The extent of a director's duty of care and skill depends to a considerable degree of the nature of the company's business and on any particular obligations assumed by or assigned to him. See *In re City Equitable Fire Insurance Co* 1925 Ch 407, 427. Compare *Wolpert v Uitzigt Properties (Pty) Ltd and others* 1961 (2) SA 257 (W) 267D–F. In that regard there is a difference between the so called full-time or executive director, who participates in the day to day management of the company's affairs or of a portion thereof, and the non-executive director who has not undertaken any special obligation. The latter is not bound to give continuous attention to the affairs of his company. His duties are of an intermittent nature to be performed at periodical board meetings, and at any other meetings which may require his attention. He is not, however, bound to attend all such meetings, though he ought to whenever he is reasonably able to do so.' See Cassim and others, *Contemporary Company Law* 557. See also Bouwman 2009 SA Merc LJ 511 and Havenga 2000 SA Merc LJ 34. Cf Bekink 2008 SA Merc LJ 100.

165 [1980] 4 All SA 525 (W) 534. See Bouwman 2009 SA Merc LJ 511 and Havenga 2000 SA Merc LJ 34. See also Bekink 2008 SA Merc LJ 100.

166 [1980] 4 All SA 525 (W) 534 the court held: 'In respect of all duties that may properly be left to some other official, a director is, in the absence of grounds for suspicion, justified in trusting that official to perform such duties honestly. He is entitled to accept and rely on the judgment, information and advice of the management, unless there are proper reasons for querying such…Obviously, a director exercising reasonable care would not accept information and advice blindly.'

professional assessments, opinions or work of professionals however such reliance is not one of blind abandon.[167]

Notably, the South African common law position adopted was inadequate and not suitable for the modern challenges that companies face where shareholders are reliant on directors to make credible, reliable and informed decisions.[168] The Institute of Directors in Southern Africa's *The King Report on Corporate Governance for South Africa 2002* (King II report), in response to the global trends, provided guidelines with respect to directors' duties of care and skill.[169] These guidelines served as a catalyst for the reform of corporate law in South Africa.[170] In 2004, the Department of Trade and Industry published a document titled *South African company law for the 21st Century: Guidelines for Corporate Law Reform.*[171] In this document it was outlined that South African corporate law did not have legislation on the duties of directors and further that corporate law jurisprudence was not aligned to the dynamic local and international business settings.[172] This led to the partial codification of directors' duties in the Act.[173]

---

167 Cassim and others*, Contemporary Company Law* 557. See Bouwman 2009 SA Merc LJ 511 and Havenga 2000 SA Merc LJ 34. See Bekink 2008 SA Merc LJ 100.

168 Cassim and others, Contemporary Company Law 558.

169 The Institute of Directors in Southern Africa, *The King Report on Corporate Governance for South Africa 2002* (the King II) 55, ch 4 para 2.3 states the following: '… must, in line with modern trends worldwide, not only exhibit the degree of skill and care as may be reasonable expected from persons of their skill and experience (which is the traditional legal formulation), but must also:

- exercise both the care and skill any reasonable person would be expected to show in looking after their own affairs as well as having regard to their actual knowledge and experience; and
- qualify themselves on a continuous basis with sufficient (at least general) understanding of the company's business and the effects of the economy so as to discharge their duties properly, including where necessary relying on expert advice.'

170 In Bekink 2008 SA Merc LJ 110, the author states, 'With the drafting of the new Companies Bill, the Legislature did in fact adhere to some of the proposals set out in the relevant King Reports and the Bill provides for a codification of director's duties as those were set out in the Reports. This includes both fiduciary duties and a duty of care, skill and diligence.'

171 Coetzee and Van Tonder 2016 Journal for Judicial Science 1.

172 Coetzee and Van Tonder 2016 Journal for Judicial Science 1. See also Department for Trade and Industry, 'South African Company Law for the 21st Century Guidelines for Corporate Law Reform'. Available at <https://www.gov.za/sites/default/files/gcis_document/201409/26493gen1183a.pdf> (date of use: 24 May 2021). At 15 it reads: 'The domestic and global environment for enterprises has changed markedly since the 1970s. Corporate structures and financial instruments have undergone significant developments. Many old concepts have been abandoned or modified and new concepts have been developed. We now live in a world of greater globalisation, increased electronic communication, greater sensitivity to social and ethical concerns, fast changing markets, greater competition for capital, goods and services. South Africa cannot afford to be left behind.'

173 Delport, *Henochsberg on the Companies Act 71 of 2008*, 295. See also Coetzee and Van Tonder 2016 Journal for Judicial Science 3. The authors explain the following: 'an interaction between

3.3 SECTION 76(3)(c) OF THE ACT

The common law duty of care and skill has been elevated with improvements with the partial codification in section 76(3)(c) of the Act.[174] Section 76(3)(c) provides that a director must carry out his or her duties with the same care, skill and diligence as is reasonably expected of a person who carries out the same duties with the same general knowledge, skill and experience as that director.

The relevant portions of section 76 of the Act read:

> 76. Standards of a director's conduct –
>
> (1) In this section, 'director' includes an alternate director, and –
>
> a) a prescribed officer; or
>
> b) a person who is a member of a committee of a board of a company, or of the audit committee of a company, irrespective of whether or not the person is also a member of the company's board…
>
> (3) Subject to subsections (4) and (5), a director of a company, when acting in that capacity, must exercise the powers and perform the functions of director –
>
> a) in good faith and for a proper purpose;
>
> b) in the best interests of the company; and
>
> c) with the degree of care, skill and diligence that may reasonably be expected of a person;
>
> i) carrying out the same functions in relation to the company as those carried out by that director; and
>
> ii) having the general knowledge, skill and experience of that director.

3.3.1 WHO OWES THE DUTY OF CARE, SKILL AND DILIGENCE?

Section 76(1)(a) and (b) of the Act determines to whom the section applies. The section applies to 'directors', 'prescribed officers' and 'board or audit committee

---

the statutory statement and the common law will exist. First, partial codification leaves room for the judiciary to fill in the gaps, with which the statutory statement does not expressly deal and, secondly, the common law must be developed as necessary to improve the realisation and enjoyment of rights established by the 2008 Act.' It is notable that partial codification presents an opportunity for development of the law within a dynamic corporate environment however where there are 'gaps', uncertainty follows which may be detrimental to directors wanting to discharge their duties in a prudent manner, see Coetzee and Van Tonder 2016 Journal for Judicial Science 6 in this regard.

174 Cassim and others, Contemporary Company Law 558.

members'. A dissection of this section is required with consideration of the definitions afforded to 'director' and 'prescribed officer' in the Act.

A 'director' is broadly defined to include a member of the board, an alternate director, a person occupying the position of director or alternate director regardless of what title they are referred to.[175] Interestingly, the definition is widely couched requiring a substantive assessment to be made when considering whether a person is a director of a company.[176]

A 'prescribed officer' is defined in regulation 38 of The Companies Regulations, 2011 as follows:

> (1) Despite not being a director of a particular company, a person is a 'prescribed officer' of the company for all purposes of the Act if that person –
>
> a) exercises general executive control over and management of the whole, or a significant portion, of the business and activities of the company; or
>
> b) regularly participates to a material degree in the exercise of general executive control over and management of the whole or a significant portion, of the business and activities of the company.
>
> (2) This regulation applies to a person contemplated in sub-regulation (1) irrespective of any particular title given by the company to –
>
> a) an office held by the person in the company;
>
> b) a function performed by the person for the company.

The regulation also affords a wide definition to determine if an individual is a prescribed officer. Board or audit committee members are included in the definition, as they have substantial influence on the decisions made by the board of directors.[177] Notably, there is no distinction drawn between an executive and non-executive director.[178] The wide

---

175 The definition of 'director' reads: 'a member of the board of a company, as contemplated in section 66, or an alternate director of a company and includes any person occupying the position of a director or alternate director, by whatever name designated.'

176 Cassim and others, *Contemporary Company Law* 404. See also Delport, *Henochsberg on the Companies Act 71 of 2008* 23 where it is explained that '[t]he title is not the determining factor to determine whether someone is a director or not.'

177 Cassim and others, *Contemporary Company Law* 511–512.

178 Contrary to the view taken by the court in *Fisheries Development Corporation of SA Ltd v Jorgensen* [1980] 4 All SA 525 (W). See the discussion under 3.2. In *Organisation Undoing Tax Abuse and another v Myeni and Others* [2020] 3 All SA 578 (GP) para 32, Tolmay J held: 'The fact that someone is a "non-executive member" does not absolve her of any legal responsibility. The legal duties of all directors are the same. These principles were summarised in *Howard v Herrigel and another NNO* where it was stated that both executive and non-executive directors are subject to the same legal duties, which include duties of care, skill and diligence. Compliance

net case with respect to the application of section 76 of the Act appears to ensure that all individuals whom have substantial control over the management of the company, regardless of their titles, are held to a standard of conduct in terms of the Act.[179]

3.3.2 SECTION 76(3)(C)(I) AND (II)

The partial codification of the common law directors' duties of care and skill is contained in section 76(3)(c) of the Act with the addition of diligence.[180] Cassim and others submit that the act 'tightens up and upgrades' the common law position.[181] It is also notable that the duty placed on directors is to the company and not the shareholders.[182] Section 76(3)(c) in relevant part states as follows:

> (3) Subject to subsections (4) and (5), a director of a company, when acting in that capacity, must exercise the powers and perform the functions of director –
>
> c) with the degree of care, skill and diligence that may reasonably be expected of a person;
>
> i) carrying out the same functions in relation to the company as those carried out by that director; and
>
> ii) having the general knowledge, skill and experience of that director.

with these duties requires an assessment of the role actually played by the director, the information available to her and the information that could have been available. If one considers the powers executed by non-executive directors, it is clearly appropriate that no distinction should be drawn between the two groups.'

179 Cassim and others, *Contemporary Company Law* 510.

180 Bouwman 2009 SA Merc LJ 513.

181 Cassim and others, *Contemporary Company Law* 558. It is noted by Delport in *Henochsberg on the Companies Act 71 of 2008* 296 that '[t]he section does not exclude the common law, and therefore the common law duties that are not expressly amended by this section or those that are not in conflict with the section will still apply.'

182 Cassim and others, *Contemporary Company Law* 559. See also *Visser Sitrus (Pty) Ltd v Goede Hoop Sitrus (Pty) Ltd* 2014 (5) SA 179 para 80. The court stated: 'Put differently, the overarching purpose for which directors must exercise their powers is the purpose of promoting the best interests of the company.' In *Hlumisa Investment Holdings (RF) Ltd and another v Kirkinis and others* [2020] 3 All SA 650 (SCA) para 52, the court held that '[the courts] are constrained to accept that a company has an established right to claim damages from its directors for any losses sustained as a result of those directors' breach of a duty owed to the company.' See also Delport *Henochsberg on the Companies Act 71 of 2008* 298(19) where it is written that '[d]irectors as such owe no fiduciary duty to the members/shareholders individually… their fundamental duty is to act only in the bona fide interests of the company and its shareholders as a body.' In *De Bruyn v Steinhoff International Holdings NV and others* [2020] JOL 47482 (GJ) para 141, the court indicated that the 'appointment to the office of director gives rise to fiduciary duties owed by a director to the company. It is the company that enforces these duties and seeks to remedy their breach. Second, there is no general fiduciary duty owed by directors to shareholders of the company. The assumption of office and the relationship between the directors and the company entails no such duty. A fiduciary duty is predicated upon a duty of loyalty. The director owes that duty to the company. And that requires the director to act in the interests of the company.'

Section 76(3)(c) of the Act requires that a director must act with the requisite degree or care, skill and diligence. The introduction of diligence to the common law duty of care and skill has been argued to extend the duty and should be read as an additional component to the duty of care and skill.[183] Van Tonder posits, referring to the definition of 'diligence' in Black's Law Dictionary, that diligence includes attendance at board meetings, attention, supervision and monitoring of the company and corporate affairs.[184] Hamadziripi and Chitimira describe diligence to connote 'caution and attention'.[185] This hints at an oversight and monitoring element of the duty of care, skill and diligence in terms of the Act.[186] Certainly, from a corporate governance point of view, the King IV under principle one recommends that directors, among other things, exercise oversight and monitoring within the corporate structure.[187] The author surmises that directors do indeed have a legislated oversight and monitoring responsibility as part of their duty of care, skill and diligence.

---

183 Van Tonder 2018 Obiter 306. The author writes: 'Section 76(3)(c) provides for the director's duty of care, skill and diligence. The word "diligence" is a new addition to the director's partially codified duty of care and skill. Arguably, this addition represents an extension of the common law duty of care and skill'. See also Van Tonder 2016 Obiter 572. See also Cassim and others, *Contemporary Company Law*, 559 where the authors opine that '[t]he wording of the section suggests that care is different from diligence.'

184 Van Tonder in 2018 Obiter 306 writes 'According to *Black's Law Dictionary* "diligence" means "[p]rudence; vigilant activity; attentiveness; or care, of which there are infinite shades, from the slightest momentary thought to the most vigilant anxiety". This would include attendances at the board and other meetings and attention to related paperwork, devoting attention to the company's affairs and the proper supervision and general monitoring of corporate affairs and policies'. See also Hamadziripi and Chitimira 2021 PER / PELJ 18.

185 Hamadziripi and Chitimira 2021 PER / PELJ 18.

186 Van Tonder 2018 Obiter 315. The author puts forward the following view: 'Section 76(3)(c) does, however, incorporate an additional standard of diligence, which, according to the definition of the word should, in principle, require of a director to diligently keep informed about the company's activities, its officers and employees and to monitor, generally, the company's affairs and policies.'

187 The Institute of Directors in Southern Africa *The King Report on Corporate Governance for South Africa 2016* (the King IV) 43. In Van Tonder 2018 Obiter 315, the author states the following: 'The broader concepts of corporate governance provide for principles and recommendations that seem to indicate that directors should actively supervise, monitor and oversee the management of the company but it is not law and does not provide guidance on the standard of conduct expected of directors in discharging their oversight function.' It is notable that s 5(1) of the Act requires that the Act must 'be interpreted and applied in a manner that gives effect to the purposes set out in section 7.' In Delport, *Henochsberg on the Companies Act 71 of 2008* 36 it is confirmed that the Act must be interpreted to give effect to the purposes of the Act. Section 7(b)(iii) of the Act states a purpose of the Act to stimulate the South African economy and growth thereof by 'encouraging transparency and high standards of corporate governance.' It may then be appropriate to suggest that a court may take into consideration the oversight standard in King IV as a means of interpreting the meaning of diligence within the context of s 76(3)(c) of the Act. See also Esser and Delport 2011 THRHR 449. The authors indicate that directors may 'have to adhere to these recommendations to prevent liability for breaching their legal duties.'

It is notable that the Act preserves the objective and subjective elements as expressed in common law, albeit in a modified form.[188] Thus, a two-legged approach is expressed by the Act. The first leg represents the objective element which sets a minimum standard by which all directors are assessed.[189] The second leg represents the subjective element which considers the director's knowledge, skill and experience.[190] Importantly, the objective standard sets a minimum threshold for the conduct of all directors which is not affected by the knowledge, skill and experience of a director.[191] Secondly, the subjective standard does not lower the minimum standard required, instead where a director has greater knowledge, is highly skilled and has tremendous experience then the level of care, skill and diligence expected is raised proportionally.[192]

3.4 THE BUSINESS JUDGMENT RULE AND SECTION 76(4) OF THE ACT

The business judgment rule originated in the United States of America (US) and was adopted by South Africa and incorporated into the Act under section 76(4).[193]

The relevant part of Section 76(4) states as follows:

---

188 Delport, *Henochsberg on the Companies Act 71 of 2008* 298(8). The author opines: 'In respect of the duty of care, skill and diligence an objective test is therefore applied to determine what the reasonable director would have done in the same situation as well as a subjective test which takes into account the general knowledge, skill and experience of the specific director'. See also Cassim and others, *Contemporary Company Law* 559.

189 Section 76(3)(c)(i) of the Act. See also Cassim and others, *Contemporary Company Law* 559 where it is written: 'The test of standard is objective to the extent that the first limb of the section, i.e. s 76(3)(c)(i), requires a director to exercise the degree of care, skill and diligence that may reasonably be expected of a person carrying out the same functions as the director. The standard is that of a reasonable person and not that of a reasonable director'.

190 Section 76(3)(c)(ii) of the Act. See also Cassim and others, *Contemporary Company Law* 559.

191 Cassim and others, *Contemporary Company Law*, 559. See also Delport, *Henochsberg on the Companies Act 71 of 2008* 298(8). See further Esser and Delport 2011 THRHR 453 and Du Plessis 2010 Acta Juridica 269.

192 Cassim and others, *Contemporary Company Law* 559. See also Delport, *Henochsberg on the Companies Act 71 of 2008* 298(8)–(9). See further Esser and Delport 2011 THRHR 453. See also Du Plessis 210 Acta Juridica 269–270. Du Plessis provides an analogy to explain the subjective element of the assessment as follows: 'Thus, the intention of the Legislature is simply to ensure that apples are compared with apples and, putting all the apples, as far as that is theoretically possible, in the same hypothetical situation comparable to the facts of the particular case!'

193 Cassim and others, *Contemporary Company Law* 563. See also Mupangavanhu 2017 Stell LR 152 and Kennedy-Good and Coetzee 2006 Obiter 64. See further Havenga 2000 SA Merc LJ 27 in which the author posits: 'The business judgment rule developed in the United States of America alongside the duty of care and relates to one aspect of this duty, namely that of decision-making.' See also Bouwman 2009 SA Merc LJ 523.

In respect of any particular matter arising in the exercise of the powers or the performance of the functions of director, a particular director of a company—

a) will have satisfied the obligations of subsection (3) (b) and (c) if—

i) the director has taken reasonably diligent steps to become informed about the matter;

ii) either—

(aa) the director had no material personal financial interest in the subject matter of the decision, and had no reasonable basis to know that any related person had a personal financial interest in the matter; or

(bb) the director complied with the requirements of section 75 with respect to any interest contemplated in subparagraph (aa); and

iii) the director made a decision, or supported the decision of a committee or the board, with regard to that matter, and the director had a rational basis for believing, and did believe, that the decision was in the best interests of the company

The business judgment rule is designed to protect a director from the risks associated with hindsight reviews of their business decisions.[194] The business judgment rule

---

194 Cassim and others, *Contemporary Company Law* 563. See Havenga 2000 SA Merc LJ 27. See also Mupangavanhu 2017 Stell LR 148, Bouwman 2009 SA Merc LJ 523, Jones 2007 SA Merc LJ 331 and Kennedy-Good and Coetzee 2006 *Obiter* 64. It is notable that the section seems to apply to any decision made or supported by the directors, s 76(4)(a)(iii) of the Act, the use of the word 'decision' seems to suggest a wider ambit of application – see Cassidy 2009 SA Merc LJ 398. It is notable that s 76(4)(b) and (5) of the Act empowers the directors to rely on external consultants, these sections are legislated as follows:

'(4) In respect of any particular matter arising in the exercise of the powers or the performance of the functions of director, a particular director of a company—

…

(b) is entitled to rely on-

(i) the performance by any of the persons-

(aa) referred to in subsection (5) ; or

(bb) to whom the board may reasonably have delegated, formally or informally by course of conduct, the authority or duty to perform one or more of the board's functions that are delegable under applicable law; and

(ii) any information, opinions, recommendations, reports or statements, including financial statements and other financial data, prepared or presented by any of the persons specified in subsection (5).

(5) To the extent contemplated in subsection (4) (b), a director is entitled to rely on-

(a) one or more employees of the company whom the director reasonably believes to be reliable and competent in the functions performed or the information, opinions, reports or statements provided;

(b) legal counsel, accountants, or other professional persons retained by the company, the board or a committee as to matters involving skills or expertise that the director reasonably believes are matters-

(i) within the particular person's professional or expert competence; or

(ii) as to which the particular person merits confidence; or

(c) a committee of the board of which the director is not a member, unless the director has reason to believe that the actions of the committee do not merit confidence'.

presents the circumstances under which a director will have satisfied his or her duty of care.[195] The practical consideration upon which the business judgment rule is based is the promotion of confident decision-making by directors without the fear of attracting liability due to hindsight review of their decisions.[196] The business judgment rule creates a rebuttable presumption that a director can rely on to avoid personal liability to the company or its shareholders for *bona fide*, though poor, decisions that negatively impact a company.[197]

At the outset it is notable that the section seems to apply to any business decision made or supported by the directors.[198] Van Tonder submits that the business judgment rule does not apply to the situation where the directors have failed to exercise their duties of oversight and monitoring (the duty of diligence) on the basis that the business judgment rule only applies in instances where the directors have made a business decision.[199] The failure to exercise oversight and monitoring duties amounts to a failure to act and does not translate to making a business decision.[200] The author submits that there must be evidence of an informed, deliberate and good faith process of decision-making undertaken by the directors for the business judgment rule to apply. This is distinct to the situation where the directors have a positive obligation and fail to act, the directors' decision not to act is not a business decision.[201]

For a director to enjoy the protection of section 76(4)(a) of the Act, there are three requirements. Firstly, the director must have made an informed decision.[202] Secondly, the director must have no personal financial interest in the decision, or alternatively

---

195 Van Tonder 2016 Obiter 574 states that '[t]he business-judgment rule thus provides the circumstances in which the duties imposed by subsection (3)(b) and (c) of the standards of directors' conduct provision, will be satisfied by a director.' See also *Visser Sitrus (Pty) Ltd v Goede Hoop Sitrus (Pty) Ltd* 2014 (5) SA 179 para 73.

196 Mupangavanhu 2017 Stell LR 153. See also Bouwman 2009 SA Merc LJ 523 and Jones 2007 SA Merc LJ 331. In Kennedy-Good and Coetzee 2006 Obiter 65–66, the authors discuss the purpose of the business judgment rule which they list as 'the encouragement of risk-taking; to persuade competent persons to undertake the office of the director; the prevention of judicial second-guessing; avoiding shareholder management in the corporation; and permitting effective market mechanisms to manage director behavior.'

197 Jones 2007 SA Merc LJ 329. See also Kennedy-Good and Coetzee 2006 Obiter 64 and 277–278.

198 Section 76(4)(a)(iii) of the Act. Van Tonder 2016 *Obiter* 577, the author refers to '[a]n action "not to take action" is also a business decision as long as the decision–making process which led to the decision that action will not be taken, was conducted in good faith and on an informed basis.'

199 Van Tonder 2016 Obiter 577. See the discussion under 3.3.2.

200 Van Tonder 2016 Obiter 577.

201 Van Tonder 2016 Obiter 577. The concept of 'positive obligations' is discussed in 4.5.3 and 5.3.3.

202 Section 76(4)(i) of the Act.

have disclosed his or her personal interest in the decision.[203] Lastly, the director must have had a rational basis for believing that the decision taken was in the best interests of the company.[204] For the purposes of this research the first and third requirements are considered in detail.[205]

The first requirement dictates that the director must have 'taken reasonably diligent steps to become informed of the matter.'[206] The assessment of steps taken to become informed is objective given the use of the phrase 'reasonably diligent steps'.[207] The directors are required to take initiative to become informed on a matter prior to taking a decision.[208] If presented with a report, they should read the report with an enquiring mind and interrogate the content with the lens of protecting and acting in the company's best interests.[209]

As the business judgment rule finds its roots in the US, a look at how the courts there have considered components of the rule is useful to convey an understanding of the manner in which the rule can be applied with respect to the first requirement of section 76 of the Act.[210] In the USA case, *Smith v Van Gorkom*,[211] a class action was brought by the shareholders of Trans Union Corporation seeking a rescission of a cash out merger of Trans Union Corporation.[212] Alternatively, damages against the board of Trans Union Corporation on the basis, among other things, that the decision made by

---

203 Section 76(4)(ii)(aa)–(bb) of the Act.

204 Section 76(4)(iii) of the Act.

205 Stevens and De Beer 2016 SA Merc LJ 257, the authors indicate 'in the absence of personal interests … the two salient requirements arising from the business judgment rule would seem to be the taking of reasonable steps to ensure a decision is informed, as well as the two-step requirement of believing a decision to be in the best interests of the company and having a rational basis for that belief.'

206 Section 76(4)(i) of the Act. See also *Organisation Undoing Tax Abuse and another v Myeni and others* [2020] 3 All SA 578 (GP) where the court indicated at para 26 that '[t]he "business judgment principle" can only protect those who act in good faith and have taken reasonable diligent steps to become informed. Willful misconduct, recklessness and dishonesty are not protected'.

207 Cassidy 2009 SA Merc LJ 399.

208 Van Tonder 2016 Obiter 576.

209 Van Tonder 2016 Obiter 576. The author indicates that '[m]ore than a passive acceptance of information presented to the board is required.' This appears to imply that a substantive and meaningful process of understanding information must be undertaken by the board so that they can stand behind the first requirement of reasonably diligent steps to become informed.

210 Section 5(2) of the Act states that a court may consider foreign law to the extent appropriate when interpreting the Act therefore it is necessary to consider how the USA jurisprudence on the application of the business judgment rule.

211 488 A.2d 858 (Del. 1985).

212 488 A.2d 858 (Del. 1985) 863.

the board for the cash out merger was not made with informed business judgment.[213] The court ruled in favour of the shareholders, citing that the directors did not act in an informed manner.[214] In arriving at the decision the court outlined that reflection on whether a director, in making a business decision, informed himself of all 'material information reasonably available to them' is necessary.[215] The information must be assessed with vigour and not for the sake of doing so.[216] The court made its findings on whether the directors were 'informed' based on an assessment of the surrounding circumstances that led to the decision.[217]

It is therefore submitted that, although the steps taken to become informed are assessed under an objective standard, the real issue is to determine what being 'informed' means. It appears that a director must be able to show that they did what was reasonable to receive information relating to a matter and demonstrate that when they received the information, they critically considered the information prior to making their business decision. In determining whether a director was 'informed', a court looks at the surrounding circumstances to assess the level of critique a director applied to the information prior to making their decision. It then may well serve directors to record their process of assessing information in order to bring certainty on the manner in which they processed the information once they received same.

The second requirement, for the purpose of this research, indicates that the director must have a rational basis to believe and did believe that their decision was in the best interest of the company.[218] The test for rationality is an objective test.[219] Cassidy submits that reasonableness and rationality are not similar.[220] Cassidy explains that although a decision may have been unreasonable, it does not automatically mean that

213 488 A.2d 858 (Del. 1985) 863–864.
214 488 A.2d 858 (Del. 1985) 864, 893.
215 488 A.2d 858 (Del. 1985) 872.
216 488 A.2d 858 (Del. 1985) 872, the court held: 'Representation of the financial interests of others imposes on a director an affirmative duty to protect those interests and to proceed with a critical eye in assessing information of the type and under the circumstances present.' Thus highlighting that the exercise of receiving and becoming informed of information required to make a business decision is not a tick box exercise but rather an immersion into such information to an extent that the director is armed to make a decision that may be considered in good faith, on an informed basis and in the best interests of the company.
217 488 A.2d 858 (Del. 1985) 874–880.
218 Section 76(4)(iii) of the Act.
219 Cassim and others*, Contemporary Company Law* 564. See also *Visser Sitrus (Pty) Ltd v Goede Hoop Sitrus (Pty) Ltd* 2014 (5) SA 179 para 76. The court held that '[t]he rationality criterion as laid down in s 76 is an objective one…'.
220 Cassidy 2009 SA Merc LJ 400.

the decision was irrational.[221] The use of rationality as the threshold of review of the directors' duties of care, skill and diligence with respect to a decision waters down the standard of conduct required of directors.[222] This then translates to a reduction in the possibility of a director who has made an unreasonable decision from being held liable for the decision on the basis that the decision was rational.[223] The rationality requirement creates a legal quagmire in that the question is, when does an unreasonable decision by a director qualify as irrational?[224] Stevens and De Beer argue that one must show that a director's decision was 'entirely baseless'.[225] Considering the facts surrounding the eventual decision, it is apparent that the director arrived at their decision in total disregard of any red flags and therefore a total failure to take care when making the decision.[226] Determination of the reliance on the business judgment rule is therefore heavily dependent on the factual matrix surrounding the conduct under question.

3.5 THE KING IV AND TECHNOLOGICAL GOVERNANCE AND SECURITY

Directors' duties, though regulated by legislation and the common law, are also guided by codes of best practice like the King IV. It is trite that non-compliance with the recommendations of the King IV does not attract liability for a director.[227] The principles outlined by the King IV can be used to assess whether directors have exercised the relevant duty of care, skill and diligence.[228] The King IV operates on an 'apply and

---

221 Cassidy 2009 SA Merc LJ 400. See also Stevens and De Beer 2016 SA Merc LJ 260.

222 Cassidy 2009 SA Merc LJ 400. See Jones 2007 SA Merc LJ 327 and 333. The author expresses the opinion regarding the business judgment rule: 'It is far more likely that it will contribute to a higher degree of corporate misconduct.' See also Stevens and De Beer 2016 SA Merc LJ 260. The authors write: 'It is submitted that this is a far more forgiving threshold than the standard of reasonableness found in the care and skill inquiry.'

223 Stevens and De Beer 2016 SA Merc LJ 261. *Visser Sitrus (Pty) Ltd v Goede Hoop Sitrus (Pty) Ltd* 2014 (5) SA 179 (WCC) para 76. The court held that 'its threshold is quite different from, and more easily met than, a determination as to whether the decision was objectively in the best interests of the company.'

224 Stevens and De Beer 2016 SA Merc LJ 262.

225 Stevens and De Beer 2016 SA Merc LJ 262. See also *Organisation Undoing Tax Abuse and another v Myeni and others* [2020] 3 All SA 578 (GP) para 26.

226 Stevens and De Beer 2016 SA Merc LJ 262 posit: 'Thus, proving irrationality would for all practical intents and purposes (specifically in terms of evidence and argument in litigation) be tantamount to proving an unreasonableness that very, very closely resembles gross negligence.'

227 Esser and Delport 2011 THRHR 449.

228 Esser and Delport 2011 THRHR 450. The authors make reference to the King III. However, it is submitted that such views also apply to later iterations as the basis of the King Reports is that directors 'should act not only in accordance with the letter of the law, but also in the spirit of their fiduciary duties' and in the best interests of the company. Interestingly, the King IV does put forward an upgraded principle-based approach as opposed to a practice-based approach by the King III, this is explained in Esser and Delport, 'The South African King IV Report on corporate

explain' approach based on the seventeen principles and associated practices, with a view to promote substantive compliance as opposed to a tick box approach.[229]

Chair of the King Committee, Mervyn King SC expressed the view that technology 'is now part of the corporate DNA'.[230] This statement fortifies the issue of security of technology being vitally important to companies given that companies are largely reliant on the technology in their daily operational running.[231] The King IV, under principle 12, suggests that the board of directors should apply their minds to the governance of information technology (IT) related issues. IT governance refers to the effective and efficient management of IT and its associated risks and costs with its use to achieve a company's objectives.[232] Therefore, the directors are tasked with the overall duty to ensure that the IT systems are aligned with the corporate objectives and that any associated risks to the company and its clients are managed adequately.[233]

Under recommended practices, the King IV requires that the directors play an active oversight role with respect to the IT management of the company.[234] The recurring requirement of directors is one of oversight. According to Van Tonder, oversight by a director refers to the duty to actively monitor, among other things, the corporate affairs of the company with the objective of avoiding harm or loss to the company.[235] A failure to discharge the duty of oversight may result in a director's liability to the company for any harm or loss suffered by the company.[236] Non-compliance with the oversight duties in the King IV may not result in liability of the director in law, however non-

governance: is the crown shiny enough?' Available at http://eprints.gla.ac.uk/163223/7/163223.pdf (date of use: 24 June 2021) 7–8.

229 The King IV 7.

230 The King IV 6.

231 Theron and Koornhof 2016 ACCC 162.

232 Theron and Koornhof 2016 ACCC 162, the authors mention that IT governance includes 'electronic privacy of customers and employees; the productive use of IT in the business structure; the protection of the online presence of business structures; protection against litigation; cyber security of business structures; the protection of intellectual property in its digital form and the management of electronic data and records in accordance with the law.' See also the King IV 6 and 62.

233 Theron and Koornhof 2016 ACCC 163.

234 The King IV 62.

235 Van Tonder 2018 Obiter 303.

236 Van Tonder 2018 Obiter 303. Van Tonder advises that the South African law on the director's duty of oversight is largely underdeveloped. He makes reference to the USA interpretation of this duty with a view to provide the context of what the duty entails and its application within a South African context.

compliance may affect the assessment of a director's liability to the detriment of the director.[237]

Particularly, it is recommended that the directors proactively monitor, identify and respond to corporate cyber breaches.[238] Directors are also advised to monitor the security of data on their systems.[239] It is notable that the recommendations accord with the requirements of the POPI Act.[240] The author submits that the additional recommendations contained in the King IV concerning cyber security demonstrates that directors must have issues related to cyber security on their radars when considering challenges that are faced by the company in the pursuance of its corporate objectives.

3.6 CONCLUDING REMARKS

This chapter has presented a discussion on the legal and regulatory framework within which directors' duties of care, skill and diligence is assessed.[241] Compliance with the duty is assessed against an objective-subjective standard.[242] Notably, the objective standard presents a minimum threshold by which all directors must abide by thus the subjective element can only increase the standard by the necessary relative level ascertained by looking at the particular education, skill and experience of the director in question.[243]

Diligence within the context of section 76(3)(c) means that directors have a legislated duty of oversight and monitoring in addition to their duties of care and skill.[244]

---

237 Van Tonder 2018 Obiter 307. See also Esser and Delport 2011 THRHR 454. The authors demonstrate, using an example of a corporate cyber breach, how the recommendations of the King III on IT governance may be used in determining if a director has complied with their duties of care, skill and diligence. See also *Minister of Water Affairs and Forestry v Stilfontein Gold Mining Co Ltd* 2006 (5) SA 333 (W) and *South African Broadcasting Corporation Ltd v Mpofu* [2009] 4 All SA 169 (GSJ), our courts have commented on the applicability and relevance of the King reports on the determination of whether directors have complied with their duties of care, skill and diligence.

238 The King IV 62.

239 The King IV 62.

240 See the discussion in 2.7.

241 See the discussions under 3.2, 3.3, 3.4 and 3.5.

242 This is discussed under 3.3.

243 See the discussion under 3.3.2.

244 This is discussed in 3.3.2.

The business judgment rule presents a legal quagmire by essentially lowering the bar further in the assessment of a director's decision.[245] The divergence of the standard of assessment between the duty of care, skill and diligence and the business judgment rule means that only decisions which are baseless may fail the test. This means that the business judgment rule effectively tempers the objective component of duty of care, skill and diligence. The enquiry into the applicability of the business judgment is heavily dependent on the factual matrix of the conduct in question.[246] Pertinent to this research is that the business judgment rule does not apply in circumstances where the directors have failed to exercise their duties of oversight and monitoring (the duty of diligence) as the business judgment rule only applies in instances where the directors have made a business decision.[247]

The King IV recommends active oversight by directors into the IT governance of the company.[248] Oversight appears to be a component of the directors' duties, finding its place under 'diligence'.[249] The King IV may then serve the purpose of founding the objective standard of care, skill and diligence required by directors with respect to IT governance.

In the next chapter, the duty of care and loyalty as well as the business judgment rule as applied in Delaware in the United States are scrutinised. The chapter examines how the courts in the United States have dealt with derivative action cases against directors for corporate cyber breaches. Moreover, the chapter provides a contextual and comparative basis upon which the duty of care and the business judgment rule is applied in Delaware courts. As South Africa has not seen any litigation related to directors' liability for corporate cyber breaches, consideration of how Delaware jurisprudence has addressed this issue is useful. It assists in conveying an understanding of how the principles of directors' duties have been applied. Perhaps South African company law can draw from the Delaware jurisprudence in the determination of liability for corporate cyber breaches.

245 See the discussion under 3.4.
246 See the discussion under 3.4.
247 See the discussion in 3.4.
248 This is discussed under 3.5.
249 This is discussed under 3.3.2 and 3.5.

CHAPTER 4 COMPARATIVE PERSPECTIVES ON DIRECTORS' LIABILITY FOR CORPORATE CYBER BREACHES IN THE USA

4.1 INTRODUCTION

In chapter two, the definition and context of corporate cyber breaches have been outlined. Thereafter, the South African legal position with respect to the duty of care, skill and diligence, the business judgment rule as well as technological governance and security in terms of King IV was discussed. The insight, in this chapter, into how the law in Delaware addresses directors' liability for corporate cyber breaches serves to provide guidance with respect to this topic within a South African context.[250] A snapshot of how the USA has dealt with liability of directors for corporate cyber breaches is presented.[251] The interpretation of the duty of oversight and monitoring in the USA jurisprudence is useful in understanding the content and extent of the comparable duty of diligence in South Africa.[252]

The duty of care and business judgment rule in Delaware is briefly explained.[253] A discussion of how the courts in the USA have decided matters related to directors' liability for corporate cyber breaches is undertaken.[254] The threshold of proof required by plaintiffs to found liability on the part of directors for corporate cyber breaches is set very high.[255] It is notable that where a positive obligation is created by law or regulation coupled with the duty of oversight and monitoring the threshold is significantly reduced and liability may be founded in this way.[256]

The comparative stances between South Africa and Delaware highlight that South African courts have not tested the duties of care, skill and diligence insofar as it relates to corporate cyber breaches.[257] The duty of diligence and the Delaware duty of oversight and monitoring appears to mirror the South African duty of diligence. Further,

250 This is discussed in 4.2.
251 See the case discussed in 4.5.
252 This is discussed in 4.5.3.
253 See the discussions under 4.3 and 4.4 respectively.
254 See the discussion in 4.5.
255 This is discussed in 4.5.1 and 4.5.2.
256 See the discussion in 4.5.3.
257 See the discussion in 4.6.

the threshold of proof required by South African law on the business judgment rule does not differ materially from the approach taken in Delaware.[258]

4.2 THE IMPORTANCE OF THE COMPARATIVE

Section 5(2) of the Act permissively provides that '[t]o the extent appropriate, a court interpreting or applying this Act may consider foreign company law'. The section permits the courts to consider foreign law when interpreting provisions within the Act.[259] Given that the business judgment rule as applied in South Africa originated in Delaware[260] and the extant active litigation in the USA related to corporate cyber breaches and directors' liability,[261] it is befitting that consideration be given to how the USA jurisdiction has dealt with this topic. South Africa is yet to see litigation with respect to corporate cyber breaches and directors' liability. Therefore, South African courts look to international jurisdictions, in terms of section 5(2) of the Act, for guidance with respect to determining whether any liability should fall on directors for corporate cyber breaches.

The approach taken, and the principles applied in terms of the corporate law of Delaware due to its status as the 'unofficial national corporate law'[262] of the USA is examined. Corporate law within the USA is state-specific.[263] As a result of the large number of companies that have been incorporated in Delaware, the development of corporate law in this state has had a significant influence on corporate law in the USA and the judicial decisions in this regard have persuasive value in other state jurisdictions within the USA.[264] The duties of directors in Delaware comprise of the duty of loyalty[265] and duty of care however, unlike South Africa, there is no separate duty of skill and diligence.[266] Interestingly, Delaware has not codified the duties

---

258 Refer to comparison in 4.6.

259 Section 5(1) of the Act states that '[t]he Act must be interpreted and applied so as to give effect to the purposes of the Act listed in section 7 of the Act'.

260 See the discussion under 3.4.

261 This is discussed in 4.5.

262 Mongalo 2016 JCCL&P 2.

263 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 1:4.

264 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 1:4. See also Mongalo 2016 JCCL&P 2.

265 The duty of loyalty is not examined in this research as it is concerned with interested director transactions where there is a conflict of interest, which falls outside the scope of this research.

266 Mongalo 2016 JCCL&P 1. See also Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:1. The South African directors' duty of care is discussed is discussed in 3.2 and 3.3.

expected of directors.[267] Under Delaware law, there exists a presumption that business decisions taken by the directors are done in accordance with their duties i.e. the business judgment rule.[268] South Africa adopted this rule for the first time in the Companies Act.[269] Delaware corporate law is therefore the most potent representation of that area of law within the USA.

4.3 THE DUTY OF CARE IN DELAWARE

The duty of care requires of directors to ensure that they are informed of all material information which is reasonably available to them when they are considering a business decision.[270] The care required of the director is that which a careful person would ordinarily use in similar circumstances.[271] The duty of care encompasses the general monitoring and oversight of the company.[272] Whether the duty of care has been complied with is a factual enquiry. The procedure the directors followed in order to reach the decision is considered in the assessment.[273]

---

267 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:3. This is unlike South Africa, where directors' duties are partially codified, as alluded to under 3.2 and 3.3.

268 Lafferty 2011 Penn St. L. Rev. 841.

269 See the discussion under 3.4.

270 Lafferty 2011 Penn St. L. Rev. 842. See also *Smith v Van Gorkom* 488 A.2d 858 (Del. 1985) 872. The court held: '[t]he determination of whether a business judgment is an informed one turns on whether the directors have informed themselves prior to making a business decision, of all material information reasonably available to them'. In Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:9. The author explains that the directors do not need to be informed of every fact. Instead, the 'board is responsible for considering only material facts that are reasonably available, not those that are immaterial or out of the board's reasonable reach'. See also Horton 40(3) Del. J. Corp. L. 936.

271 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:5. See also Furlow 2009 Utah L. Rev. 1063, 1069.

272 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:1 reads: '[t]he duty of care requires a director to act in good faith and on an informed basis in arriving at a business decision. It includes the responsibility of the director to oversee the activities of the corporation by attending directors' meetings, by requiring that the company provide adequate information upon which to make decisions, by carefully reviewing the documentation which is provided, and through general oversight and monitoring of management'. See also McNeill and Frank 2019 Am. Bankr. L.J. 651.

273 Palm and Kearney 1995 Vill. LR 40 1307. See also Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:9. The author explains that '[t]he amount of diligence or inquiry necessary to make an "informed" decision is necessarily dependent upon the particular circumstances of the case, including the magnitude of the transaction at issue and the knowledge and expertise of the particular directors and officers involved'. Further, the author indicates that '[a]t a minimum, the board of directors should insist that adequate information concerning all important matters requiring board attention be distributed to the board in time to permit a review of the information before any vote is taken'. The importance of the process taken by the directors in their decision-making cannot be underestimated as much scrutiny is placed on the process by the judiciary in determining if the directors have exercised the necessary care prior to making a business decision.

In the landmark decision of *Smith v Van Gorkom*,[274] the shareholders brought an action against the directors after they had agreed to and approved the sale of the company at a price considerably lower than its value.[275] The court considered the board of directors' duty of care and held that directors can attract liability for business decisions that are made in an unconsidered manner.[276] So, if directors did no more than accept the information provided to them without question or without careful analysis then the directors could be held liable to the company or shareholders should the decision lead to a claimable event. The court considered procedural factors such as the amount of time spent by the directors deliberating the sale and the directors' failure to use external expert advice.[277] In the assessment of the directors' business decision, the court held:

> The directors (1) did not adequately inform themselves as to Van Gorkom's role in forcing the 'sale' of the Company and in establishing the per share purchase price; (2) were uninformed as to the intrinsic value of the Company; and (3) given these circumstances, at a minimum, were grossly negligent in approving the 'sale' of the Company upon two hours' consideration, without prior notice, and without the exigency of a crisis or emergency.

In response to *Smith v Van Gorkom,*[278] the legislature under section 102(b)(7) of the Delaware General Corporation Law[279] enacted what is known as an exculpatory provision.[280] The section eliminates a director's personal liability for a breach of the duty of care should the exculpatory provision be included in the company's certificate of incorporation. The exculpatory provision does not provide absolute protection in that claims based in breach of loyalty and bad faith fall outside the ambit of the provision.

Notably, the directors' duty of care encompasses the duty of oversight.[281] *In re Caremark International Inc. Derivative Litigation*[282] spoke to the assessment of directors' duty of care with respect to oversight. In this matter the shareholders alleged that the directors did not put in place appropriate and adequate internal controls to

---

274 488 A.2d 858 (Del. 1985). This case is discussed under 3.4.
275 488 A.2d 858 (Del. 1985) 863.
276 488 A.2d 858 (Del. 1985) 863–864.
277 488 A.2d 858 (Del. 1985) 874–880.
278 488 A.2d 858 (Del. 1985).
279 Title 8, Chapter 1, Delaware Code. See also Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:12.
280 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:10.
281 This is comparable to the 'diligence' element of the duty of care, skill and diligence in South Africa. This is discussed under 3.3.2.
282 698 A.2d 959 (Del. Ch. 1996).

prevent employees from committing criminal offences.[283] These offences resulted in the company incurring fines and penalties thus causing a financial loss to the company.[284] The issue, therefore, was whether the directors had paid an appropriate level of attention to the possibility of these offences being committed by the employees. The following questions were devised in order to determine the directors' liability; (1) whether the directors were aware, or whether they should have been aware, of the risk, (2) whether they had taken the necessary steps in good faith in order to prevent or correct the risk; and (3) whether a causal link existed between their failure to take steps and the loss suffered by the company.[285] The standard set by this case created a high threshold for a plaintiff to meet in order to prove that the directors breached their fiduciary duty of care (relating to oversight) in this regard.[286]

Delaware courts have applied a standard of gross negligence when considering if the directors have breached their duty of care in that the directors showed a wilful disregard, reckless abandon or the company and shareholders alternatively have made a decision with no rational reasoning.[287] It is submitted that such a standard creates a lower watermark against which a director may be deemed to have complied with the duty of care.

4.4 THE BUSINESS JUDGEMENT RULE

The business judgment rule is the presumption that a business decision made by a director was done so free from personal interest, in the good faith and with due care.[288] According to the rule, the directors must have made the business decision on an informed basis, in good faith and in the honest belief that the decision is in the best interests of the company.[289]

---

283 698 A.2d 959 (Del. Ch. 1996) 964.

284 698 A.2d 959 (Del. Ch. 1996) 964.

285 698 A.2d 959 (Del. Ch. 1996) 971. See also Ackerman 2019 Wayne St. UJ Bus. L. *2* 17.

286 Ackerman 2019 Wayne St. UJ Bus. L. *2* 17.

287 Lafferty and others 2011 Penn St. L. Rev. 116 843. See also Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:9. In *Smith v Van Gorkom* 488 A.2d 858 (Del. 1985) 873, the court confirmed the view that 'the concept of gross negligence is also the proper standard for determining whether a business judgment reached by a board of directors was an informed one'. In Horton 40(3) Del. J. Corp. L. 936, the author affirms that 'merely bad decisions do not violate the duty of care. Instead the management's decision must rise to the level of gross negligence'.

288 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:16.

289 In *Aronson v Lewis* 473 A.2d 805 (Del. 1984) 812, the court explained that the business judgment rule 'is a presumption that in making a business decision the directors of a corporation acted on

The rule, much like its South African counterpart,[290] limits a director's liability by stifling the hindsight judicial review of a business decision taken by a director.[291] To successfully rebut the business judgment rule presumption, it must be shown that the directors were grossly negligent in the exercise of their duty of care in respect to a business decision.[292] The business judgment rule also does not apply to the directors' oversight and monitoring duties.[293] In this regard it bears relevance to quote the court from *In re Walt Disney Co. Derivative Litigation*[294]:

> Furthermore, in instances where directors have not exercised business judgment, that is, in the event of director inaction, the protections of the business judgment rule do not apply.[295]

Accordingly, inaction by directors does not amount to a business decision that was a result of an informed, deliberate and good faith decision process. In the result the business judgment rule is not applicable.[296]

4.5 JURISPRUDENCE ON SHAREHOLDER DERIVATIVE ACTION AGAINST DIRECTORS FOR CORPORATE CYBER BREACHES IN THE USA

4.5.1 PALKON EX REL. WYNDHAM WORLDWIDE CORP. V HOLMES 907 A.2D 693 (DEL. CH. 2005)

Palkon ex re Wyndham Worldwide Corp. v. Holmes[297] (*Palkon*) was a shareholder derivative action claim against the directors of Wyndham Worldwide Corporation

---

an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company'. See also *In re Walt Disney Co. Derivative Litigation* 906 A.2d 27 (Del. 2006) 52 in which the court held that '[o]ur law presumes that "in making a business decision the directors of a corporation acted on an informed basis, in good faith, and in the honest belief that the action taken was in the best interests of the company." Those presumptions can be rebutted if the plaintiff shows that the directors breached their fiduciary duty of care or of loyalty or acted in bad faith. If that is shown, the burden then shifts to the director defendants to demonstrate that the challenged act or transaction was entirely fair to the corporation and its shareholders'.

290 The application of the business judgment rule in South Africa is discussed under 3.4.

291 Colombo, 'Law of Corporate Officers and Directors: Rights, Duties and Liabilities', § 2:16. In Furlow 2009 Utah L. Rev. 1083, the author explains that '[b]usiness decisions require boards to make judgments about the future of corporations. Because the future is uncertain, directors cannot be held to a standard that would subject them to personal liability for decisions that turn out badly. The business judgment rule allows boards to take calculated business risks without fear of incurring personal liability'.

292 Palm and Kearney 1995 Vill. LR 1307. Interestingly, this is similar to the South African position (as discussed under 3.4), however it is not as clearly expressed compared to Delaware jurisprudence.

293 This is discussed in 3.4.

294 907 A.2d 693 (Del. Ch. 2005).

295 at 748.

296 See the discussion under 3.4.

297 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014).

(WWC) as a result of three data breaches between 2008 and 2010.[298] The breaches resulted in the personal and financial details of 600 000 customers being taken by cyber criminals.[299] The breaches prompted the Federal Trade Commission (FTC) to investigate the breaches which resulted in legal action against WWC. The plaintiff then issued a demand on the board of WWC to 'investigate, address, and promptly remedy the harm inflicted' on WWC, however the board of WWC declined the plaintiff's demand.[300] Despite ignoring the demand, the board of WWC engaged in several meetings on the topics of cyber-attacks, security policies as well as security enhancements.[301] Security firms were appointed, and their recommendations were implemented.[302]

In response to the declination of their demand, the plaintiff filed a derivative lawsuit against WWC and related parties (the defendants).[303] The plaintiff alleged that the board failed in their oversight duty to implement proper and adequate measures to prevent the corporate cyber breaches.[304] The plaintiff further alleged that consequent to the data breach, the company incurred significant legal costs as well as suffered reputational damage.[305] The plaintiff alleged further that refusal of their demand was wrongful.[306]

In response to the allegations, the defendants moved to dismiss the action by the plaintiff averring that the refusal of the demand was an exercise of business judgment in good faith and after due diligence, further that even if the refusal was wrongful the

298 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 2.

299 Ackerman 2019 Wayne St. UJ Bus. L. 2 18. In *Palkon* the use of the word 'taken' can be explained by the following description from the court, 'On three occasions between April 2008 and January 2010 that information was stolen. Hackers breached WWC's main network and those of its hotels. They performed a 'brute force attack,' which means they guessed user IDs and passwords to enter an administrator's account, and then used 'memory-scraping malware' to collect sensitive data. Through these methods, the hackers obtained the personal information of over six-hundred thousand customers.'

300 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 3.

301 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 3 and 4.

302 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 4.

303 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 4.

304 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 4, the court, in detailing the facts indicated '[a]t the heart of Plaintiff's complaint is an assertion that Defendants failed to implement adequate data-security mechanisms, such as firewalls and elaborate passwords, and that this failure allowed hackers to steal customers' data'.

305 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 4.

306 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 4.

plaintiff had not stated their claim properly and that the plaintiff's damages were 'speculative and unripe'.[307]

In considering the allegations of the plaintiff, the court undertook an examination of the business judgment rule as applied in Delaware.[308] The court summarised the legal position with respect to the business judgment rule as a presumption that the directors, when making a business decision did so 'on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company'.[309] Therefore, in order to rebut the presumption, the plaintiff was required to show that the WWC board had made the decision in bad faith or by unreasonable investigation, which the court noted was a 'high burden' of proof.[310]

In the courts assessment on whether the plaintiff demonstrated that the WWC board's decision to refuse their demand was in bad faith, the court explained that the plaintiff was required to demonstrate that the board's refusal of the demand could not be categorised as a sound business decision and its only rationale was bad faith.[311] The court did not believe that the plaintiff had succeeded in proving that the WWC board's refusal was based in bad faith.[312] On whether the investigation conducted by the board was unreasonable, the court explained that the plaintiff had to allege that the defendants were grossly negligent in that the decision was made on scant information in an 'unintelligent and unadvised' manner.[313] The court explained that the defendants in this case had been familiar with issues related to cyber-attacks before the plaintiff issued his demand.[314] The court placed attention on the facts that suggested the board

307 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 4. The plaintiff (at 5) refuted these averments which the court summarised as follows: 'He first contends that the Board wrongfully refused his demand by relying on an investigation dominated by conflicted counsel. He next urges that he adequately pleaded his legal claims, as WWC failed to institute reasonable security protections. Last, Plaintiff asserts that shareholders have already suffered damages due to the costs of defending against the FTC investigation'.

308 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 5. The court examined the derivative action process available to shareholders as a means to bring legal action on behalf of the company. The court considered that the demand is a step in the derivative action process and a decision to abide or not falls under the purview of business judgment.

309 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 5.

310 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 6.

311 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 6.

312 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 6–9.

313 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 9.

314 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 9.

was sufficiently informed on issues of cyber-attacks, given the content of their meetings and past investigations.[315]

The court dismissed the plaintiff's lawsuit on the basis that the business decision to refuse the plaintiff's demand was protected by the business judgment rule as the decision was made in good faith and after conducting a reasonable investigation.[316]

At first glance, *Palkon* primarily concerned the board's refusal of the plaintiff's demand. On further inspection, it is submitted that the court's comments regarding the application of the business judgment rule can be extended to the expectations with respect to the duty of care *vis-à-vis* oversight.[317] It is submitted that demonstrating a business decision's only rationale is bad faith is a stretch for a plaintiff. The assessment is *ex post facto* and not *ex ante,* so due consideration must be given the exact circumstances that were present when the decision was made, therefore no armchair critical speculative opinions can be imputed to the circumstances.[318] It then follows that the factual matrix which illustrates the steps taken by the board to become informed plays an integral component to the assessment. It is apparent that the enquiry takes a form over substance stance on whether the directors exercised their business judgment in a manner that would exonerate them for not taking complete steps to prevent cyber breaches. Further, *Palkon* seems to suggest there should have been an absolute blatant disregard of the risks. Thus, it seems, even the weakest of considerations by a director could absolve him or her from liability.

4.5.2 IN RE HOME DEPOT, INC. SHAREHOLDER DERIVATIVE LITIGATION 223 F. SUPP. 3D 1317 (N.D. GA. 2016)

In re Home Depot Inc. Shareholder Derivative Litigation 223 F. SUPP. 3D 1317 (N.D. GA. 2016) (*In re Home Depot*) concerned a corporate cyber breach that led to the theft of personal financial data of 56 million Home Depot customers.[319] The breach occurred

315 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 9-11. The court made mention of the General Counsel brief every quarter on the breaches and general cyber related issues. Previous investigations meant that the board was sufficiently informed of the issues that underpinned the plaintiff's demand.

316 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 9. See also Ackerman 2019 Wayne St. UJ Bus. L. 2 20.

317 Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014) 5-11.

318 In *Palkon* the court presented a clear fact-based decision. The court did not stray from the factual matrix.

319 223 F. Supp. 3d 1317 (N.D. Ga. 2016) 1321.

over a period of time in 2014 where the cyber criminals used a third-party username and password to breach the security system.[320] The estimated cost of the breach to the company was USD 10 billion. This was a shareholder derivative action wherein it was alleged, among other things, that the board breached their duty of loyalty in that they failed to implement adequate internal controls to oversee the risks that the company would encounter as a result of a corporate cyber breach.[321] In response to the allegations, the defendants moved to dismiss the claim against them.[322]

In the assessment of whether the directors breached their duty of loyalty, the court considered the allegations made by the plaintiffs in this regard.[323] First, the plaintiffs alleged the failure of the board to appoint anyone to oversee data security after disbanding the Infrastructure Committee (IC) and failing to amend the Audit Committee (AC) charter to include the data security duties of the IC.[324] In doing so, there was no reporting system in place.[325] On this allegation, the court ruled that that such formality did not delegitimise the AC's inherited IC data security duties as the AC and the board were aware and recognised the transfer.[326] It was further expressed that by the plaintiffs' own version, the board received data security management reports from the AC, so there could be no basis to say that a reporting system did not exist.[327]

A further allegation made by the plaintiffs was that the board of directors did not have a plan in place immediately to correct deficiencies in Home Depot's data security.[328] The key issue with this allegation as expressed by the court was that the plaintiffs were not saying that there was no plan in place but rather that the plan the board agreed on to address deficiencies was simply not good enough.[329] The court explained that the plaintiff would have to demonstrate that the board had knowingly and completely

320 *In re Home Depot* 1320 and 1321.
321 *In re Home Depot* 1321. The plaintiffs alleged further that '[a]s a result of their alleged failure to take the risk of a data breach seriously and immediately implement security measures, the Breach occurred'.
322 *In re Home Depot* 1323.
323 *In re Home Depot* 1325–1327.
324 *In re Home Depot* 1326.
325 *In re Home Depot* 1326.
326 *In re Home Depot* 1326. The court indicated that '[w]hether or not the Audit Committee had technical authority, both the Committee and the Board believed it did'.
327 *In re Home Depot* 1326. In this regard the court made the point that '[i]mportantly, the Plaintiffs repeatedly acknowledge that there *was* a plan, but that in the Plaintiffs' opinion it moved too slowly'.
328 *In re Home Depot* 1326.
329 *In re Home Depot* 1326.

derogated from their duty.[330] The court noted further that where the directors have taken reasonable action to address a specific issue then it cannot be said that they did not exercise their duty of loyalty.[331] The court further highlighted that bad faith on the part of the directors cannot be inferred simply because the directors' actions were unsatisfactory.[332] The court indicated that the plan the directors had, although it was not perfect, was enough for them to discharge their duty of loyalty.[333] Importantly, the court expressed the view that the directors' plans need not be perfect but rather reasonable.[334]

It is submitted that in *In re Home Depot* further illustrates the lengths to which plaintiffs must prove that the directors should not be protected by the business judgment rule. Although, the court acknowledged that the directors did not implement the plan that they devised quickly enough, which would have mitigated the corporate cyber breaches, the court still found that the directors did not act contrary to their duty of loyalty.[335] It is submitted further that this matter also demonstrates a form over substance approach to the assessment of whether directors have discharged their duties without liability attaching to them.

4.5.3 IN RE FACEBOOK, INC. SECTION 220 LITIGATION CONSOLIDATED C.A. NO. 2018-0661-JRS (DEL. CH. MAY. 30, 2019)

In re Facebook, Inc. Section 220 Litigation Consolidated C.A. No. 2018-0661-JRS (Del. Ch. May. 30, 2019) (*In re Facebook*) is a fairly recent matter involving facts in which Facebook suffered a data breach in 2015 which was not disclosed to its users.[336] The breach occurred when a consulting firm, Cambridge Analytica, poached the private data of 50 million users.[337] In July 2018, Facebook's share value was reduced by USD 120 billion after news reports of the breach were made public.[338] As a

330 *In re Home Depot* 1326. This line of reasoning is aligned with the general high threshold of proof that a plaintiff must meet in order to prove that a director breached their duties of loyalty and care within Delaware jurisprudence. See the discussion outlined in 5.5.1.
331 *In re Home Depot* 1326.
332 *In re Home Depot* 1326. The court, referring to Delaware law, stated '[r]ather, they use language like "utterly" and "completely" to describe the failure necessary to violate the duty of loyalty by inaction.'
333 *In re Home Depot* 1327.
334 *In re Home Depot* 1327.
335 *In re Home Depot* 1327.
336 *In re Facebook* 2.
337 *In re Facebook* 2.
338 *In re Facebook* 2.

contextual background, in 2011, Facebook was subject to a consent decree issued by the Federal Trade Commission (FTC) on the basis that Facebook's data security measures were inadequate and they needed 'more robust and verifiable data security protocols'.[339] It was discovered after news of the breach that Facebook was dealing in user data without their consent and consequently, various federal and international agencies initiated investigations into the data protection activities of Facebook.[340]

Pursuant to the breach, Construction and General Building Labourers, the plaintiff served a demand on Facebook requiring access to the company's books and records with the view to investigate, among other things, whether there were any fiduciary breaches by the directors of the company.[341] In response, Facebook alleged that the plaintiff had failed to found a credible basis upon which it could be said that the directors breached their duty of oversight as the corporate cyber breach was unanticipated and levelled against their existing and adequate data security measures.[342] It is notable that the In re Facebook matter related specifically to whether the plaintiff's demand to inspect the books and records of Facebook was valid in the circumstances.[343] In finding in favour of the plaintiffs, there are key aspects that the court comments on with respect to the directors' breach of their duty of oversight that is pertinent to this research.

The court specifically referred to the consent decree issued by the FTC to Facebook, wherein a positive obligation was placed on the company to improve their data security measures.[344] In this regard, the court explains that the liability for a breach of oversight is easily ascertainable where there is a positive duty placed on the directors and they fail to discharge that duty.[345] The court explained further that the law does not protect law breakers. In the result, liability will befall the directors when they act contrary to the law.[346] A key point highlighted by the court is that a director cannot claim they are

339 *In re Facebook* 2.
340 *In re Facebook* 2.
341 *In re Facebook* 3.
342 *In re Facebook* 3.
343 *In re Facebook* 5.
344 *In re Facebook* 42. The court refers to the consent decree as an 'affirmative obligation imposed on the [c]ompany much like positive law'.
345 *In re Facebook* 42.
346 *In re Facebook* 43.

loyal to the company where they are allowing the company to violate the law.[347] The author agrees with the court's reasoning related to positive obligations presenting an efficient means of determining whether the directors have breached their duties of oversight.

In South Africa, the duty of oversight and monitoring is encapsulated within the duty of diligence.[348] The question then begs are the "positive obligations" of the duty of diligence ascertainable from the surrounding prevailing environmental conditions? In other words, can it be said that directors have an oversight and monitoring obligation within a South African context to prevent corporate cyber breaches given the increased risk[349] of such breaches? The author submits that the answer is in the positive.[350]

4.6 COMPARATIVE STANCES BETWEEN SOUTH AFRICA AND THE USA

South Africa is yet to see litigation related to the liability of directors for corporate cyber breaches as compared to the USA. It is submitted that our law is yet to test directors' duties of care, skill and diligence insofar as it relates to corporate cyber security.

The Delaware courts have considered the question of a director's duty of care specifically against their oversight and monitoring duties.[351] This is comparable to the duty of diligence, introduced to section 76(3)(c) of the Act, which the author submits is a legislated duty of oversight and monitoring.[352]

With respect to the business judgment rule, Delaware jurisdiction requires that a plaintiff crosses a high threshold to demonstrate that the director cannot rely on the business judgment rule on the basis of their gross negligence.[353] In South Africa, the

---

347 *In re Facebook* 43 and 44. The court states that the directors 'must act in good faith to ensure that the corporation tries to comply with its legal duties'.

348 See discussion under 3.3.2 on the inclusion of 'diligence' as part of the duty of care.

349 This is discussed in 2.6.

350 Interestingly in *In re Facebook* 43, see fn 150 where the court explains '[i]n other words, it is more difficult to plead and prove Caremark liability based on a failure to monitor and prevent harm flowing from risks that confront the business in the ordinary course of its operations. Failure to monitor compliance with positive law, including regulatory mandates, on the other hand, is more likely to give rise to oversight liability'. The author submits the increased risk of corporate cyber breaches (see the discussion in 2.6), legislation related to IT risks (refer to the discussion in 2.7) and the King IV (see the discussion in 3.5) may be relied on to found the 'positive obligations' within the context of the duty of diligence.

351 See the cases discussed in 4.5.

352 The inclusion of 'diligence' in s 76(3)(c) of the Act is discussed in 3.3.2.

353 This is discussed in 4.4, 4.5.1 and 4.5.2.

view is much the same in that it must be shown that the director arrived at their decision in total disregard of any red flags.[354] Importantly, the business judgment rule does not apply in instances where the directors have failed in their oversight and monitoring duties.[355]

Do these comparisons provide foresight into how our courts may deal with questions of diligence and the application of the business judgment rule with respect to corporate cyber breaches? Could the form over substance approach taken by the Delaware courts be at odds with the purposeful interpretation required by the Act in South Africa?[356] We may yet see these questions answered in the years to come as litigation with respect to corporate cyber breaches in South Africa is initiated.

4.7 CONCLUDING REMARKS

This chapter provides a snapshot of directors' duty of care[357] as well as the application of the business judgment rule[358] in Delaware, USA. The duty of care includes the duty of oversight and monitoring of the company which is comparable to the duty of diligence required by the Act in South Africa.[359]

A discussion of notable decisions in the USA concerning corporate cyber breaches illustrates the high threshold a plaintiff must cross in order to demonstrate that a director has breached their duty of care (oversight and monitoring). The analysis of application of Delaware corporate law on the point of 'positive obligations' has presented the basis for the author's view that the increased risk of corporate cyber breaches, legislation related to IT risks and the King IV may be relied on to found the

354 See the discussion under 3.4.
355 This is discussed in 4.4.
356 See fn 187 for a discussion on the purposeful interpretation required by the Act when courts are interpreting the Act. In Delport, *Henochsberg on the Companies Act 71 of 2008* 54(1) it is stated: that '[i]n respect of the provisions of sub-s (a) the application of foreign company law in terms of s 5(2) should be carefully considered as to the similarity between the bases of the constitutional dispensation in the different jurisdictions'. The author submits that the form over substance assessment taken by the Delaware courts may be at odds with s 7(b)(iii) of the Act that states one of the purposes of the Act is to stimulate the South African economy and growth thereof by 'encouraging transparency and high standards of corporate governance.' Corporate governance with respect to corporate cyber security (see the discussion under 3.5) require an active application of mind to issues of IT management by directors, thus favouring a substantive approach.
357 Discussed in 4.3.
358 This is discussed in 4.4, 4.5.1 and 4.5.2.
359 See discussion in 4.3 and 4.6.

'positive obligations' within the context of the duty of diligence in South Africa.[360] The significance of this view is presented in the next chapter.[361]

It is submitted that the form over substance view taken by the Delaware courts with respect to corporate cyber breaches is not appropriate within the South African context as it is at odds with purposes of the Act and principles of corporate governance.[362]

In the next chapter, the nature of and basis for the liability of directors for a breach of their duty of care, skill and diligence in terms of the Act is scrutinised. The purpose of the analysis is to determine whether, and if so, on what basis directors may be held liable for corporate cyber breaches in South Africa. The chapter comprises of an assessment of the duty of care, skill and diligence as well as the possible reliance of directors on the business judgment rule within the South African context.

360 This is discussed in 4.5.3 and fn 350.
361 See the discussion under 5.3.3.
362 See discussion in 4.5.2, wherein the form over substance approach by the courts in the USA is highlighted.

CHAPTER 5 THE BASIS FOR LIABILITY OF DIRECTORS FOR A BREACH OF THE DUTY OF CARE, SKILL AND DILIGENCE

5.1 INTRODUCTION

It has been submitted that where a company suffers a corporate cyber breach and suffers a loss,[363] then such loss may be claimable from the directors on the basis that the directors have breached their duties of care, skill and diligence.[364] In the preceding chapters, the nature and content of directors' duties of care, skill and diligence has been discussed.[365] As there is no litigation and precedent on the topic in South Africa and given the permissive interpretive mandate on courts to consider foreign law when interpreting the Act, Delaware jurisprudence has been considered on a comparative basis to South Africa.[366] The comparative analysis yielded that a form over substance application of facts to the question of whether the directors have discharged their duties of care, skill and diligence is not appropriate in South African company law.[367] However, the consideration of 'positive obligations' created by law and regulation as a means to found the basis of liability may prove to be useful. This is discussed more fully in this chapter.[368]

With the law on the directors' duties of care, skill and diligence illustrated,[369] this chapter considers the basis upon which a director may be held liable for a breach of their duty of care, skill and diligence within the context of corporate cyber breaches.[370] In terms of section 77(2)(b)(i) of the Act, a director may be held liable in delict for a breach of section 76(3) of the Act.[371] A brief explanation is provided with respect to derivative actions in terms of section 165 of the Act.[372] The elements of delict as well as their application within the context of directors' duties are discussed.[373] Notably, it

363 This is discussed in 2.7.
364 See the discussion in 3.2.
365 This is discussed in ch 3.
366 This is discussed in ch 4.
367 See the discussion under 4.7. In this regard, s 5(2) of the Act begins with 'to the extent appropriate'.
368 This is discussed in 5.3.3.
369 See the discussion under 3.3.
370 See the discussions under 5.2 and 5.4. This chapter answers the question posed by this research as to whether directors in South Africa may be held liable for damages suffered by the company as a result of a corporate cyber breach.
371 This is discussed under 5.2.
372 See the discussion under 5.2.
373 This is discussed under 5.3.

is established that where a statute provides a delictual remedy for a breach, then a breach will be sufficient to found delictual wrongfulness.[374] With respect to negligence, the standard of duty of care against which a director's actions should be assessed is discussed.[375] Section 218(2) of the Act is also considered in relation to its applicability as a remedy for a breach of a director's duty of care, skill and diligence.[376]

5.2 BREACH OF THE DUTY OF CARE, SKILL AND DILIGENCE IN TERMS OF SECTION 77(2)(b)(i) OF THE ACT

If a company falls victim to a corporate cyber breach and suffers damages then the company may sue the directors of the company in delict on the basis that they breached their duties of care, skill and diligence.[377] The Act speaks to the liability of directors and prescribed officers in section 77. The relevant part of section 77 reads as follows:

> (2) A director of a company may be held liable –
>
> b) in accordance with the principles of the common law relating to delict for any loss, damages or costs sustained by the company as a consequence of any breach by the director of—
>
> i) a duty contemplated in section 76 (3) (c);
>
> ii) any provision of this Act not otherwise mentioned in this section; or
>
> iii) any provision of the company's Memorandum of Incorporation.

At first glance it is notable that the section applies to loss, damages and costs suffered by the company only. The implication is that all other stakeholders do not fall within the ambit of section 77(2)(b)(i) of the Act. This further confirms that the duty of care, skill and diligence is owed only to the company by the directors.[378] In this regard, it is then necessary to briefly discuss section 165 of the Act.

374 This is discussed under 5.3.2.
375 See the discussion under 5.3.3.
376 Discussed under 5.4.
377 This is discussed in 5.1.
378 See the discussion under 5.3.2.

Section 165 of the Act abolished the common law derivative action[379] and introduces a statutory form of the derivative action.[380] The derivative action is available to various categories of applicants, among others to shareholders, directors, trade unions and employee representatives and persons granted standing by a court.[381] Section 165 of the Act empowers any of these categories of applicants to serve a demand on the company to institute, sustain or take any related steps with the objective of protecting the company's legal interests.[382] On receipt of the demand the company may, within fifteen days, make an application to court to have the demand set aside on the basis that it is frivolous or vexatious.[383] Alternatively, within a period of sixty days, the company may decide to abide by the demand by either instituting, sustaining or taking related steps to protect the legal interests described in such demand or notify the applicant of its refusal to abide by the demand.[384] The applicant who has made a demand to the company may apply to the court for leave to institute or sustain proceedings on behalf of and in the name of the company.[385]

Section 77(2)(b)(i) of the Act specifically relates to a breach of the duty of care, skill and diligence. The section indicates that the liability of a director who breaches the

---

379 Coetzee 2010 Acta Juridica 292. The author indicates that '[t]he derivative action can be described as a unique remedy because it allows a person to bring an action that belongs to someone else'. In Cassim 2014 SA Merc LJ 2, Cassim provides a succinct explanatory note on the rationale of the derivative action as follows: 'The derivative action is designed, first, as a remedial device by which shareholders may enforce rights or recover compensation for the company when the board of directors refuses to do so and, secondly, as a deterrent device to prevent management abuse and to ensure control over the board by allowing shareholders and others to litigate against directors who have breached their fiduciary duties to the company'.

380 Section 165(1) of the Act. Also see Cassim and others, *Contemporary Company Law* 778 and Delport, *Henochsberg on the Companies Act 71 of 2008* 596(1).

381 Section 165(2) of the Act. Also see Cassim and others, *Contemporary Company Law* 779.

382 Section 165(2) of the Act. In *Hlumisa Investment Holdings (RF) Ltd and another v Kirkinis and others* [2020] 3 All SA 650 (SCA) para 32, the court held that '[i]n a situation where wrongdoers themselves control the company, so that they can prevent the taking of the necessary steps, any one or more of its members may bring what is known as a derivative action, that is, an action by an individual shareholder, in own name, against the wrongdoers for relief to be granted to the company, the action being one on the company's behalf'. See also Coetzee 2010 Acta Juridica 298. The author explains that the use of the phrase 'legal interests' is not defined by the Act and 'could consequently be interpreted very widely'.

383 Section 165(3) of the Act.

384 Section 165(4)(b)(i) and (ii) of the Act.

385 Section 165(5) of the Act. It is notable that the derivative action only allows an applicant to pursue proceedings on behalf of and in the name of the company. This is important in that it aligns with ss 76(3) and 77(2)(b)(i) in that both these sections refer specifically to the company only. With respect to s 165(5) of the Act, a discussion on the reasons why a court may grant such application falls wide of the ambit of this research. In terms of s 165(5)(b)(i)(ii) and (iii), a court may grant the application if the court is satisfied that the applicant is acting on good faith, the proceedings demanded relate to a 'serious question of material consequence to the company', and it is in the best interests of the company for the applicant to be granted such leave as pleaded.

duty of care, skill and diligence may be found liable under the principles of delict. According to Neethling and Potgieter, a delict is 'the act of a person that in a wrongful and culpable way causes harm to another'.[386] There are five elements which must be proved before the conduct complained of can be considered to be a delict.[387] They are: an act (conduct) must have been performed, the conduct must have been wrongful, the perpetrator must have been at fault and there must have been a causal link between the act performed and harm suffered.[388]

5.3 THE ELEMENTS OF DELICT IN THE CONTEXT OF A BREACH OF SECTION 76(3)(c) OF THE ACT

An understanding of the content and application of each of the elements of delict within the context of a director's breach of the duty of care, skill and diligence is essential. The five elements are: conduct, wrongfulness, fault, causation and harm.[389] Where a plaintiff is able to demonstrate that all five elements are present, then the defendant is found liable in delict.[390] Below, each element of delict is analysed against the context of a corporate cyber breach.

5.3.1 CONDUCT

Conduct refers to the voluntary act or omission of a human which resulted in the harm causing event.[391] Although 'conduct' is delineated as either a commission or an omission, liability for an omission is generally more difficult to establish as the law does not easily impute a legal duty on an individual to do something to prevent harm befalling another.[392] Neethling and Potgieter postulate that the distinction between a commission and omission makes no difference in relation to the issue of conduct.[393] It is submitted that this view is correct especially given that the material question with respect to the element of conduct is whether harm was caused by the conduct of the

386 Neethling and Potgieter, *Law of Delict* 4.
387 Neethling and Potgieter, *Law of Delict* 4.
388 Neethling and Potgieter, *Law of Delict* 4.
389 Neethling and Potgieter, *Law of Delict* 4.
390 Neethling and Potgieter, *Law of Delict* 4.
391 Neethling and Potgieter, *Law of Delict* 7–8.
392 Neethling and Potgieter, *Law of Delict* 32.
393 Neethling and Potgieter, *Law of Delict* 32. The authors refer to Van der Walt and Midgley, *Principles of Delict*, 92 and quote the following pertinent point: 'The mere fact that the linguistic alternatives enable us to describe the positive occurrence in a negative way (for example, "driver failed or omitted to stop at the stop street") is legally irrelevant in the determination of the nature of the conduct'.

defendant? The conduct, regardless of whether it is a commission or omission, must have caused the damage being claimed.[394]

Therefore, it is submitted that within the context of a director's duties of care, skill and diligence one may argue that the failure to oversee and implement appropriate plans with the necessary monitoring mechanisms in order to prevent damages befalling the company, either in the form of reputational costs or reduced share value, may be sufficient to constitute conduct (an omission) as envisaged by the law of delict. Applying this line of thinking to the situation of damages caused to the company as a result of a corporate cyber breach, it would be sufficient for a plaintiff to simply allege that the directors failed to act in accordance with their duties of care, skill and diligence in terms of the Act in that they did not monitor and oversee the company's cyber infrastructure and as a result the company suffered damages.

5.3.2 WRONGFULNESS

Even though the defendant's conduct may have caused damage, the conduct must also be wrongful.[395] Wrongfulness refers to the infringement of the plaintiff's 'legally protected interest' in a 'legally reprehensible manner'.[396] In *Roux v Hattingh*[397] the court reaffirmed the context of the element of wrongfulness by quoting a passage from the Constitutional Court matter of *Le Roux v Dey:*[398]

> In the more recent past our courts have come to recognise, however, that in the context of the law of delict: (a) the criterion of wrongfulness ultimately depends on a judicial determination of whether – assuming all the other elements of delictual liability to be present – it would be reasonable to impose liability on a defendant for the damages flowing from specific conduct; and (b) that the judicial determination of that reasonableness would in turn depend on considerations of public and legal policy in accordance with constitutional norms. Incidentally, to avoid confusion it should be borne in mind that, what is meant by reasonableness in the context of wrongfulness has nothing to do with the reasonableness of the defendant's conduct [which is part of the element of negligence], but it concerns the reasonableness of imposing liability on the defendant for the harm resulting from that conduct.[399]

---

394 Neethling and Potgieter, *Law of Delict* 7. It must be noted that for a delict all elements (conduct, wrongfulness, fault, causation and harm) must be present.

395 Neethling and Potgieter, *Law of Delict* 35. It goes without saying that in the absence of wrongfulness, a defendant cannot be held liable in delict.

396 Neethling and Potgieter, *Law of Delict* 35.

397 [2013] JOL 30335 (SCA) para 33.

398 2011 (3) SA 274 (CC).

399 2011 (3) SA 274 (CC) para 122.

The assessment of wrongfulness is objectively considered after the fact, taking into account the relevant facts, circumstances and consequences that occurred after the defendant's conduct.[400] Within the context of statutory duties, breach of such duties may be *prima facie* wrongful.[401] Notably, statutory provisions may empower those protected by it with delictual actions should the provision be breached by those it imposes legal duties.[402] In these circumstances it is submitted that imposing liability on a defendant is reasonable given that the statute specifically refers to delictual action against the defendant. It is submitted in circumstances where statute imposes a delictual remedy for a breach then such breach is sufficient to found delictual wrongfulness.[403]

Within the context of a breach of the duty of care, skill and diligence, it is notable that there is no doubt that this is a legislated duty. Breach of such a duty attracts liability in terms of section 77(2)(b)(i) of the Act in terms of delict. It is, therefore, submitted that where it is alleged that the defendant breached the duty of care, skill and diligence then wrongfulness is established.

Within the context of this research, it is submitted that it is sufficient for a plaintiff to rely on the fact that the Act imposes a statutory duty of care, skill and diligence on directors therefore a breach of such legal duty would meet the element of wrongfulness.

---

400 Neethling and Potgieter, *Law of Delict* 35. This research specifically focuses on the assessment of wrongfulness within the context of a breach of statutory duty.

401 Neethling and Potgieter, *Law of Delict* 90.

402 Neethling and Potgieter, *Law of Delict* 75 and 90.

403 In Neethling and Potgieter, *Law of Delict* 91 and 92, the authors refer to McKerron, *The Law of Delict* 257 and outline considerations which may point to wrongful conduct in the context of a breach of statutory obligation. The considerations are listed as follows:

'(a) that the relevant statutory measure provided the plaintiff with *a private law* remedy;
(b) that the plaintiff is a person for whose benefit and protection the statutory duty was imposed;
(c) that the nature of the harm and manner in which it occurred are such as are contemplated by the enactment;
(d) that the defendant in fact transgressed the statutory provision; and
(e) that there was a causal nexus between the transgression of the statutory provision and harm.'

Following on from the above, it is submitted that where a statute specifically provides a Plaintiff with its remedy in delict, and the claim made by the Plaintiff is one that arises directly from a breach of the statute for harm the statute was enacted to protect the Plaintiff from, then such breach of statute may then be considered unlawful for the purposes of founding delictual wrongfulness. One can conclude that in such a circumstance that it is reasonable to impose liability on the defendant by virtue of the statute specifically indicating that a breach of the statute attracts liability in delict.

5.3.3 FAULT

After the determination of wrongfulness, one must consider if the defendant's conduct falls within the parameters of delictual fault.[404] There are two forms of fault recognised in our law, namely negligence (*culpa)* and intention (*dolus).*[405] This is referred to as the subjective element of the test for delict although the test for negligence is objective.[406]

The negligence of the defendant's conduct is objectively considered against the standard of the reasonable person (the *bonus paterfamilias).*[407] The test for negligence was outlined in the preeminent South Africa case, *Kruger v Coetzee*[408]*.* The court stated:

> For the purposes of liability *culpa* arises if-
>
> a) *diligens paterfamilias* in the position of the defendant-
>
> i) would foresee the reasonable possibility of his conduct injuring another in his person or property and causing him patrimonial loss; and
>
> ii) ii) would take reasonable steps to guard against such occurrence; and
>
> b) the defendant failed to take such steps.[409]

Within the company law context, the Act preserves the common law delictual action.[410] It bears importance to discuss who is a *diligens paterfamilias* (known as a reasonable person). A reasonable person is a fictitious person by whom conduct is measured objectively.[411] A reasonable person is the 'legal personification' of the qualities that society at large expects of people who interact every day.[412] The characteristics of the

---

404 In Neethling and Potgieter, *Law of Delict* 155, the authors explain the decision to determine fault or wrongfulness first is 'controversial'. They conclude by indicating that a court determines which of these elements to consider first based on the circumstances of the matter before it.

405 Neethling and Potgieter, *Law of Delict* 155. This research focuses primarily on negligence (*culpa)*.

406 Neethling and Potgieter, *Law of Delict* 155.

407 Neethling and Potgieter, *Law of Delict* 164.

408 [1966] 2 All SA 490 (A).

409 [1966] 2 All SA 490 (A) 491.

410 Section 77(2)(b)(i) of the Act.

411 Neethling and Potgieter, *Law of Delict* 169, the authors describe the reasonable person as 'not an exceptionally gifted, careful or developed person; neither is he underdeveloped, nor someone who recklessly takes chances or who has no prudence.'

412 Neethling and Potgieter, *Law of Delict* 169.

reasonable person are dynamic and contemporary with the prevailing environmental conditions.[413] On this note, Neethling and Potgieter submit:

> [C]ircumstances such as improved technology and improved access to education, training and information may require the reasonable person to be more stringent in evaluating the degree of care expected of human conduct in particular circumstances.[414]

It is, therefore, submitted that the level of severity of the duty of care required of a reasonable person is considered against all surrounding factors that existed when the conduct complained off occurred.[415]

With respect to the reasonable foreseeability and preventability components of the test a brief discussion is warranted to outline the content of these components. Reasonable foreseeability requires consideration of the probability of the harm complained off occurring, therefore if the probability of harm occurring was high then it can be concluded that such harm was foreseeable.[416]

Reasonable preventability of harm evaluates whether the defendant took reasonable steps to prevent the reasonably foreseeable harm from occurring.[417] It is notable that even if the defendant took steps and the harm still occurred, this does not mean that such steps were unreasonable.[418]

Neethling and Potgieter referring to *Pretoria City Council v De Jager*[419] outline the factors considered by the courts in the assessment of the reasonability of the preventative steps taken by a defendant:

---

413 Neethling and Potgieter, *Law of Delict,* 170. See also Ahmed 2021 PER / PELJ 14, the author explains that '[t]he reasonable person test is flexible and adaptable in that the courts adapt the standard depending on the circumstances of each case'. The use of the word environmental conditions is used to denote the general surrounding circumstances both physical and theoretical.

414 Neethling and Potgieter, *Law of Delict* 170.

415 Midgley 2000 Acta Juridica 89–90. See also *Cape Metropolitan Council v Graham* [2001] 1 All SA 215 (A) paras 8 to 15 where the court undergoes an assessment of the prevailing surrounding facts and environmental conditions to determine the objective standard of the reasonable person in the circumstances so that the court could assess the culpability of the appellant.

416 Neethling and Potgieter, *Law of Delict* 179.

417 Neethling and Potgieter, *Law of Delict* 180.

418 Neethling and Potgieter, *Law of Delict* 180.

419 1997 (2) SA 46 (A) 55–56.

> (i) The degree or extent of the risk created by the actor's conduct; (ii) the gravity of the possible consequences if the risk of harm materialises; (iii) the utility of the actor's conduct; and (iv) the burden of eliminating the risk of harm.[420]

The assessment is factual (*ex post facto*) and considers the above quoted factors against the standard of the reasonable person in the circumstances and whether such reasonable person would have taken reasonable preventative steps.[421]

To overcome the enquiry into the director's exercise of duty of care, skill and diligence under the assessment of negligence, the director may rely on the statutory business judgment rule by showing that they took reasonably diligent steps to become informed about the matter under consideration and had a rational basis to believe that their decision was in the best interests of the company.[422] It bears special mention that the rationality requirement has the effect of watering down the standard of conduct required by the director to the extent that an unreasonable decision may be deemed rational, in which case the director may find protection under the business judgment rule.[423] Importantly, the business judgment rule only applies to circumstances where a business decision is made and not for mere failures to act.[424]

In this research, it has been established that section 76(3)(c)(i) and (ii) of the Act requires that a director must act with the requisite degree or care, skill and diligence.[425] A two-legged approach, formulated as an objective and subjective assessment, is used to assess if a director has discharged their duties of care, skill and diligence.[426] The objective leg assesses the director's conduct against that of a reasonable person carrying out the same functions in the company as the director in question.[427] It is submitted that the first leg considers the minimum standard of conduct required of the director taking into account the particular surrounding facts of the complained conduct. In other words, the reasonable person standard must be ascertained for the particular

---

420 Neethling and Potgieter, *Law of Delict* 181. See also *Cape Metropolitan Council v Graham* [2001] 1 All SA 215 (A) para 7, *Bergrivier Municipality v Van Ryn Beck* 2019 (4) SA 127 (SCA) para 49, and *Naidoo v Minister of Police and others* [2015] 4 All SA 609 (SCA) para 25.

421 Neethling and Potgieter, *Law of Delict* 184.

422 See the discussion under 3.4 on the business judgment rule.

423 This is discussed in detail in 3.4.

424 See the discussion under 3.4.

425 This is discussed under 3.3.2.

426 This is discussed in 3.3.2.

427 Section 76(3)(c)(i). See also Van Tonder 2016 Obiter 568, the author states '[t]he standard provided for is that of a reasonable person, but ultimately takes cognizance of the fact and links the reasonable person in the situation to a reasonable director with the words "carrying out the same functions in relation to the company as those carried out by that director"'.

situation against which the director's conduct would be measured. Applying these principles to the current research, it is notable that corporate cyber breaches are undeniably a global issue. The risk posed to businesses across the world and in South Africa have been widely publicised and data protection and cybercrimes have taken center stage in South Africa.[428] Therefore, a reasonable person in the position of the director carrying out the same functions is required to be 'more stringent in evaluating the degree of care expected of human conduct'[429] with respect to corporate cyber issues. Importing the concept of 'positive obligations'[430] to the South African context, it is submitted that, objectively viewed, there is a minimum standard of diligence (oversight and monitoring) required by directors with respect to corporate cyber issues.[431] It is submitted that 'positive obligations' of oversight and monitoring have been established due to the increased risk of corporate cyber breaches[432], legislation related to IT risks[433] and the King IV.[434] The author, therefore, submits that a minimum standard by which all directors can be assessed with respect to corporate cyber issues is easily determinable in terms of the first leg of section 76(3)(c)(i).[435]

On the relevant aspects of reasonable foreseeability of preventability, the author submits that it cannot be denied that harm to the company as a result of a corporate

---

428 This is discussed in 1.1, 2.6 and 2.7. See also Ngqakamba 'Justice department's IT system brought down in ransomware attack'. Available at https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909 (Date of use: 9 September 2021). A cyber breach was detected in the form of ransomware on the system at the Department of Justice and Constitutional Development. In Toyana 'Cybersecurity: South African companies are ripe for hackers'. Available at https://www.dailymaverick.co.za/article/2021-08-01-cybersecurity-south-african-companies-are-ripe-for-hackers/ (Date of use 9 September 2021) wherein the cyber breach at Transnet SOC Ltd in July 2021 is discussed along with the far-reaching consequences that such breach had on the marine industry and related companies. The Virgin Active South Africa data breach was widely publicised and further emphasises the relevance of corporate cyber breaches, in this regard see https://hello.virginactive.co.za/assist/cyber-attack (Date of use: 9 September 2021). See also Nieselow 'Five massive data breaches affecting South Africans' Mail & Guardian Online Available at https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/ (Date of use: 9 September 2021). The author outlines major data breaches that occurred in South Africa between 2017 and 2018. These were corporate cyber breaches suffered by South African based companies with the exception of Facebook. It is submitted that there can be no doubt that the 'reasonable person' would be aware of the importance and impact of corporate cyber breaches and accordingly evaluate the required degree of care.

429 See fn 414.

430 Discussed under 4.5.3.

431 This is discussed in 4.5.3 and fn 350.

432 See the discussion in 2.6.

433 See the discussion in 2.7.

434 See the discussion in 3.5.

435 This is discussed in 3.3.2.

cyber breach is reasonably foreseeable.[436] In relation to reasonable preventability, consideration is given to the magnitude of the risk of harm and whether, objectively viewed, any steps taken would be onerous to the reasonable person.[437] Thus, if the burden of taking steps to prevent the harm outweighs the gravity of the risk then a reasonable person would not take preventative steps.[438] It is submitted that the magnitude of the risk of a corporate cyber breach is far-reaching and the reasonable person would take steps to prevent the potential harm to the company.[439] Failure to discharge the duties of oversight and monitoring means that the directors do not meet the objective standard and therefore are in breach of their duty of care, skill and diligence in term of the Act.[440]

With respect to the second leg, the subjective assessment, consideration is given to the knowledge, skill and experience of the directors however this assessment does not reduce the minimum standard ascertained in the first leg.[441] Therefore, if the director has an IT-related background both in education and career experience then such profile would serve to place a greater burden on the director in their exercise of care, skill and diligence on corporate cyber issues.

The question then arises whether a director can rely on the business judgment rule as a safe harbor to escape liability if the director is found to have acted in breach of their duty of care, skill and diligence? It is submitted that the directors cannot rely on the business judgment rule where they have failed to exercise their duties of oversight and monitoring.[442] However, in the event that the facts show that the directors undertook an informed, deliberate and good faith decision-making process and a business decision was made which led to a corporate cyber breach, then there may be an argument to be made that the business judgment rule may apply and an assessment into the rationality of such decision would depend on the factual matrix of the matter.[443]

---

436 The harm that a company can suffer due to a corporate cyber breach is discussed in ch 2.
437 Neethling and Potgieter, *Law of Delict* 184.
438 Neethling and Potgieter, *Law of Delict* 184.
439 The financial impact of a corporate cyber breach is discussed in 2.4. In 2.7 it is explained that the financial impact on South African companies as a result of a corporate cyber breach is R2.14 million which can lead to the liquidation of a company.
440 Section 76(3)(c)(i) of the Act.
441 This is discussed in 3.3.2.
442 This is discussed in 3.4.
443 See the discussion in 3.4.

5.3.4 CAUSATION

There must be a causal nexus between the defendant's conduct and the damage.[444] Therefore, if the defendant's conduct did not cause damage then there can be no delict.[445] This is known as factual causation and it is determined by the use of the *condition sine qua non* test (also known as the 'but for' test).[446] This test requires that an enquiry be made whether, but for the defendant's conduct, the damage would have occurred.[447] If the assessment is in the affirmative then the defendant's conduct is not sufficiently linked to the damage and therefore there is no delictual causation.[448]

Where the damage is too remote from the conduct of the defendant then such damage should not be imputed onto the defendant.[449] The determination of the remoteness of damage is assessed by considering legal causation.[450] Legal causation asks if the damage claimed is sufficiently linked to the conduct of the defendant for the damage to be imputed on the defendant based on 'reasonableness, fairness and justice'.[451] Notably, the question of legal causation does not arise in every matter.[452]

Within the context of this research, the determination of causation is dependent upon whether any of the damage claimed was in fact caused by a corporate cyber breach which resulted from the directors' breach of the duties of care, skill and diligence.

5.3.5 DAMAGES

An action in delict is compensatory in nature.[453] Therefore, the plaintiff must have suffered a loss of some kind, either patrimonial or non-patrimonial, for which they wish to be compensated.[454] Patrimonial losses can be expressed in monetary value and refer to a plaintiff's subjective rights.[455] Non-patrimonial are not expressed in monetary

444 Neethling and Potgieter, *Law of Delict* 215.
445 Neethling and Potgieter, *Law of Delict* 215.
446 Neethling and Potgieter, *Law of Delict* 217.
447 Neethling and Potgieter, *Law of Delict* 219.
448 Neethling and Potgieter, *Law of Delict* 219.
449 Neethling and Potgieter, *Law of Delict* 231.
450 Neethling and Potgieter, *Law of Delict* 230.
451 Neethling and Potgieter, *Law of Delict* 234.
452 Neethling and Potgieter, *Law of Delict* 232. The question of legal causation arises in situations where it is not apparently clear from the facts whether certain damages are sufficiently linked to the defendant's conduct. In the absence of such uncertainty, then the establishment of factual causation will be sufficient.
453 Neethling and Potgieter, *Law of Delict* 255.
454 Neethling and Potgieter, *Law of Delict* 255.
455 Neethling and Potgieter, *Law of Delict* 263.

terms and refer to the plaintiff's personality rights.[456] In both instances, the plaintiff bears the onus of proving their loss and quantum of such loss on a balance of probabilities.[457]

Within the context of company law, it is, therefore, submitted that the company must prove its loss and associated quantum on a balance of probabilities. Where a company suffers a loss in share value then such loss is patrimonial in nature as the shares relate to the subjective rights of the company and can be expressed in monetary value.[458] Damage to reputation however may be deemed non-patrimonial as it relates to the personality rights of the company and cannot readily be reduced to a monetary value.[459]

Where a company claims for damage as a result of a corporate cyber breach then those damages may include costs of containment and investigation, regulatory and legal costs, loss of share value, brand or reputational costs, claims from customers or vendors as well as any other costs that can be shown to be attributed to the corporate cyber breach.[460]

5.4 LIABILITY IN TERMS OF SECTION 218(2) OF THE ACT

Section 218(2) of the Act states:

> Any person who contravenes any provision of this Act is liable to any other person for any loss or damage suffered by that person as a result of that contravention.

Upon further inspection, a few aspects stand out in this section. The section imputes liability on any person who contravenes any section of the Act for the resultant loss or damage to another person. In the *Hlumisa Investment Holdings (RF) Ltd and another v Kirkinis and others*,[461] the court considered the nature and extent of section 218(2) of the Act against the backdrop of shareholders claiming for reflective losses for a drop in share value due to the directors breaching section 76(3) of the Act.[462] In its analysis, the court reaffirmed that the duties outlined in section 76(3) were owed by the directors

456 Neethling and Potgieter, *Law of Delict* 288.
457 Neethling and Potgieter, *Law of Delict* 287 and 299.
458 See fn 455.
459 See fn 456.
460 The financial impact of a corporate cyber breach is discussed in 2.4.
461 [2020] 3 All SA 650 (SCA) paras 41–52.
462 [2020] 3 All SA 650 (SCA) para 1.

to the company only.[463] The liability for breach of such duties by the directors is provided for under section 77(2)(a) and (b) of the Act specifically.[464] By providing for a specific remedy to the company for a breach of section 76(3) of the Act, the Legislature is clear on where liability should lie for conduct by directors as well as who could recover the resultant loss.[465] It is submitted that this judgment confirms that in circumstances where the company suffers any damage or loss as a result of a breach of section 76(3)(c) of the Act then liability may only be found in terms of section 77(2)(b) in delict *vis-à-vis* the directors. So, in the instance where a company suffers a diminution in share value as a result of an unreasonable and irrational business decision made by the directors, the company's action against the directors for such damage must be referred under section 77(2)(b) of the Act only.

It is submitted that claims for damages as a result of a corporate cyber breach may only be brought against the directors by the company, alternatively on a derivative basis in terms of section 165 of the Act.

5.5 CONCLUDING REMARKS

In this chapter the basis of liability of directors for a breach of the duty of care, skill and diligence within the context of corporate cyber breaches has been examined. Section 77(2)(b)(i) of the Act provides that a breach of directors' duties of care, skill and diligence is determined in terms of the principles of delict.[466] Therefore, it must be shown that the conduct complained of was wrongful, negligent and causally connected to the damage being claimed.[467] The five elements of delict are: conduct, wrongfulness, fault, causation and harm.[468] Importantly, it is only the company who may seek to hold the directors liable for breaching their duties.[469]

To found the element of conduct, it is sufficient for a plaintiff company to allege that a corporate cyber breach resulted due to the failure of the directors to oversee and monitor the company's cyber infrastructure.[470]

---

463 [2020] 3 All SA 650 (SCA) para 48.
464 [2020] 3 All SA 650 (SCA) para 48.
465 [2020] 3 All SA 650 (SCA) para 50.
466 See the discussion in 5.2.
467 This is discussed in 5.2 and 5.3.
468 See the discussion under 5.3.
469 This is discussed in 5.2 and 5.4.
470 See the discussion in 5.3.1.

On the element of wrongfulness, the author submits that it is sufficient for the plaintiff company to allege a breach of the statutory duty of care, skill and diligence as such breach is *prima facie* wrongful.[471]

Fault relates to the question of negligence within the context of this research. In terms of the Act there is an objective and subjective, two-legged enquiry implied to determine if the directors have breached their duties of care, skill and diligence.[472] The objective leg requires that an assessment of the directors' conduct be measured against the conduct of the reasonable person in the position of the director under the relevant circumstances, the subjective leg only becomes relevant in cases where the director in question has special skills or experience.[473] The key aspect is that the attributes and conduct of the reasonable person are determined against the prevailing environmental conditions. Therefore, within the context of this research, this means that the reasonable person is aware of the corporate cyber issues, specifically the threat of corporate cyber breaches and accordingly take the necessary reasonable preventive steps.[474] Notably, it is submitted that certain 'positive obligations' establish a minimum standard of diligence (oversight and monitoring) required of directors with respect to corporate cyber issues.[475]

The business judgment rule protects directors for their rational, though unreasonable, business decisions thus serving as a defence to allegations of negligence.[476] It is submitted by the author that the 'positive obligations' with respect to oversight and monitoring duties of directors (the duty of diligence) do not fall within the ambit of a business decision and the directors cannot rely on the business judgment rule to escape liability where they have failed to discharge this duty.[477]

---

471 This is discussed in 5.3.2.

472 See the discussion under 5.3.3.

473 This is discussed in 5.3.3.

474 See the discussion in 5.3.3.

475 See the discussion under 5.3.3. Also refer to the discussion in 2.7 where the obligations of a company in terms of the POPI Act are discussed with respect to the protection of customer data. Ultimately, the directors must ensure that the company complies with the duty. It is submitted that a 'positive obligation' of oversight and monitoring rests on company directors.

476 This is discussed in 5.3.3.

477 See the discussion in 5.3.3.

Causation is established where the plaintiff company can demonstrate a sufficient link between the damage claimed and the breach of the directors' duties of care, skill and diligence.[478]

Damages must be proved by the plaintiff company in that the company must show that it either suffered a patrimonial or non-patrimonial loss as a result of a corporate cyber breach which could be a drop in share value or brand value.[479]

It is submitted that the directors may be held liable by the company for breach of their duties of care, skill and diligence as a result of a corporate cyber breach where such breach can be attributed to poor oversight and monitoring by the directors of the corporate cyber infrastructure. It is submitted further that the directors cannot rely on the business judgment rule as a safe harbour from liability as the duties of oversight and monitoring do not fall within the ambit of business decisions which are capable of such protection.[480]

478 Refer to the discussion under 5.3.4.
479 This is discussed in 5.3.5.
480 See the discussion under 5.3.3.

CHAPTER 6 CONCLUSION AND RECOMMENDATIONS

6.1 INTRODUCTION

The purpose of this research was to convey an understanding of the importance of corporate cyber breaches as a potential liability risk for directors. Further, the research aimed to establish whether and, if so, on what basis directors can be held liable to the company for damages that result from a corporate cyber breach on the basis that they have failed to discharge their duties of care, skill and diligence in terms of Act. The research also aimed to postulate how delictual liability may be founded in terms of section 77(2)(b)(i) of the Act and to answer the question of whether liability may be avoided by the directors by relying on the business judgment rule. Lastly, this research aimed to provide possible recommendations to directors on how they may mitigate potential liability to the company for damages caused as a result of a corporate cyber breach. These objectives have been achieved as more fully explained in this chapter.

This research establishes that directors can be held liable for corporate cyber breaches in South Africa. The nature and content of 'diligence' as envisaged in section 76(3)(c) of the Act means that directors have a positive duty of oversight and monitoring.[481] This duty does not involve the exercise of business judgment. Oversight and monitoring are positive duties required by directors as a matter of course.[482] This positive duty of oversight and monitoring extend to corporate cyber matters due to the increased risk of corporate cyber breaches, legislation related to IT risks and the King IV.[483] As a result of the failure to discharge their duty of oversight and monitoring, the directors may be held liable in terms of section 77(2)(b)(i) of the Act in delict.[484] Directors cannot rely on the business judgment rule to escape liability for a failure to exercise oversight and monitoring with respect to corporate cyber matters as such failure does not stem from the exercise of a business decision.[485]

In this chapter the outcomes of the objectives of this research are ventilated. The questions posed in the research are answered: whether corporate cyber breaches are a potential liability risk for directors, on what basis can directors be held liable to the

481 This is discussed in 3.3.2 and 4.5.3.
482 See the discussion in 3.4.
483 This is discussed in 5.3.3.
484 This is discussed in ch 5.
485 See the discussions under 3.4 and 5.3.3.

company for damages that result from a corporate cyber breach, how delictual liability may be founded in terms of section 77(2)(b)(i) of the Act and whether liability may be avoided by the directors by relying on the business judgment rule. Recommendations in respect of what directors may do to mitigate potential liability are put forward.

6.2 CORPORATE CYBER BREACHES AS A POTENTIAL LIABILITY RISK FOR DIRECTORS.

It has been established in Chapter 2 that the corporate cyber breaches cannot be underestimated by directors as it is a top risk to the further existence of the company.[486] The South African judiciary have acknowledged the potential threat of cyber criminals to companies, and further the increased reliance of companies on conducting business on cyber networks.[487] Contemporary legislation in South Africa relating to cyber issues, namely the POPI Act and the Cybercrimes Act, impose positive obligations of oversight and monitoring on companies to comply with the duties in terms of these acts, specifically the protection of personal information as well reporting corporate cyber breaches to the relevant authorities.[488] It is submitted that corporate cyber issues enjoy pride of place on the liability risk radar of directors.

6.3 THE BASIS OF DIRECTOR LIABILITY FOR CORPORATE CYBER BREACHES, DELICTUAL LIABILITY AND THE BUSINESS JUDGMENT RULE

Director liability for a breach of the duty of care, skill and diligence in terms of the Act may be found in delict.[489] Therefore, the directors' liability is assessed against the five elements of delict—conduct, wrongfulness, fault, causation and harm.[490] Notably, the element of fault (negligence or intent) requires an assessment of the directors' conduct from an objective and subjective point of view.[491] It has been established that a reasonable person in the position of a director carrying out the same functions is required to be 'more stringent in evaluating the degree of care expected of human conduct with respect to corporate cyber issues'.[492] Failure to discharge the duties of oversight and monitoring means that the directors do not meet the objective standard

---

486 See the discussions in 2.4, 2.5, 2.6 and 2.7.
487 See the discussion under 2.6.
488 Refer to the discussion in 2.7.
489 This is discussed in ch 5.
490 See the discussion in 5.3.
491 This is discussed in 5.3.3.
492 See the discussion in 5.3.3. Neethling and Potgieter, *Law of Delict,* 181 referring to *Pretoria City Council v De Jager* 1997 (2) SA 46 (A) 55–56.

and therefore are in breach of their duty of care, skill and diligence in term of the Act.[493] The business judgment rule has been ruled out as a remedy which can be relied on by the directors to escape liability where they have failed to exercise their duties of oversight and monitoring.[494]

6.4 RECOMMENDATIONS FOR DIRECTORS TO MITIGATE THEIR POTENTIAL LIABILITY FOR CORPORATE CYBER BREACHES

It has been established that directors have a general duty of oversight and monitoring as part of their composite duties of care, skill and diligence in terms of the Act and common law in South Africa.[495] Therefore, it is essential for directors to fully understand what their oversight and monitoring duties are with respect to corporate cyber issues. It is recommended that directors review the relevant legislation[496] to consider their obligations, plot their level of risk and devise the relevant risk mitigation, oversight and monitoring plans. It may be suitable for the directors to consult with third-party consultants. However, such reliance does not delegate their potential liability to such third-party consultant for a corporate cyber breach.[497] Third-party consultants may provide expert advice on the weak points of the corporate cyber infrastructure which may be susceptible to cyber threats thus mitigating potential corporate cyber breaches and the related losses. It is further recommended that a robust reporting, oversight and monitoring system is designed and implemented to ensure that corporate cyber-related matters are interrogated or brought to the attention of the directors on a scheduled and urgent basis. Consideration should be given to the appointment of a cyber-security committee that must include members of the board and suitably qualified committee members whose task is to solely address corporate cyber issues, the intention being that these issues are given priority within the list of pertinent matters requiring the boards' attention.

493 See the discussion in 5.3.3.
494 This is discussed in 5.3.3.
495 This is discussed in ch 3.
496 See the discussion under 2.7.
497 See fn 194.

6.5 CONCLUSION

Given the extraordinary increase of corporate cyber breaches within South Africa and the world, it is clear that corporate cyber issues require robust and intentional actions by directors, who are tasked with the management of the company.[498] It has been established that directors have an oversight and monitoring duty with respect to corporate cyber issues and therefore when a corporate cyber breach occurs, their potential for liability is dangerously high as they may not be able to rely on the business judgment rule to come to their rescue.[499] As a result, directors can no longer rely on their ignorance with respect to corporate cyber issues being passed off as a poor decision thus excusing them from liability. The dynamic nature of corporate law demands greater care, skill and, most of all, diligence from directors to manage the corporate cyber matters of companies failing which liability will befall those directors.

498 This is discussed in ch 2.
499 This is discussed in ch 3 and 5.

BIBLIOGRAPHY

Table of Bills and Statutes

Companies Act 71 of 2008.

Companies Act 61 of 1973.

Cybercrimes Act 19 of 2020.

Protection of Personal Information Act 4 of 2013.

Table of Cases

SA

Absa Bank Ltd v Companies and Intellectual Property Commission and Others 2013 (4) SA 194 (WCC).

Bergrivier Municipality v Van Ryn Beck 2019 (4) SA 127 (SCA).

Boschpoort Ondernemings (Pty) Ltd v ABSA Bank Ltd 2014 (2) SA 518 (SCA).

Cape Metropolitan Council v Graham [2001] 1 All SA 215 (A).

De Bruyn v Steinhoff International Holdings NV and others [2020] JOL 47482 (GJ).

Fisheries Development Corporation of SA Ltd v Jorgensen [1980] 4 All SA 525 (W).

Fourie v Van der Spuy and De Jongh Inc 2020 (1) SA 560 (GP).

Hlumisa Investment Holdings (RF) Ltd and another v Kirkinis and others [2020] 3 All SA 650 (SCA).

Kruger v Coetzee [1966] 2 All SA 490 (A).

Le Roux v Dey 2011 (3) SA 274 (CC).

Naidoo v Minister of Police and others [2015] 4 All SA 609 (SCA).

Organisation Undoing Tax Abuse and another v Myeni and others [2020] 3 All SA 578 (GP).

Rabinowitz v Van Graan and Others 2013 (5) SA 315 (GSJ) (26 April 2013).

Roux v Hattingh [2013] JOL 30335 (SCA).

S v Msomi 2020 (1) SACR 197 (ECG).

Visser Sitrus (Pty) Ltd v Goede Hoop Sitrus (Pty) Ltd 2014 (5) SA 179 (WCC).

UK

In re Elgindatahad Ltd [1991] BCLC 959 Ch.

Re Brazilian Rubber Plantations and Estates Ltd [1911] Ch 425.

Re Denham & Co (1884) LR 25 Ch D 752.

Re Equitable Fire Insurance Co Ltd [1925] Ch 407.

Turquand v Marshall (1868-69) LR 4 Ch App 376.

US

Aronson v Lewis 473 A2d 805 (Del. 1984).

In re Caremark International Inc. Derivative Litigation 698 A.2d 959 (Del. Ch. 1996).

In re Facebook, Inc. Section 220 Litigation CONSOLIDATED C.A. No. 2018-0661-JRS (Del. Ch. May. 30, 2019).

In re Home Depot, Inc. S'holder Derivative Litig. 223 F. Supp. 3d 1317 (N.D. Ga. 2016).

In re Walt Disney Co. Derivative Litigation 906 A.2d 27 (Del. 2006).

In re Walt Disney Co. Derivative Litigation 907 A.2d 693 (Del. Ch. 2005).

Palkon ex re Wyndham Worldwide Corp. v. Holmes Civil Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014).

Smith v Van Gorkom 488 A.2d 858 (Del. 1985).

Text and Reference Books

Caravelli and Jones, *Cyber Security: Threats and Responses for Government and Business*

> Caravelli J and Jones N, *Cyber Security: Threats and Responses for Government and Business* (Santa Barbara, California, Praeger, An Imprint Of Abc-Clio, Llc 2019)

Cassim and others, *Contemporary Company Law*

> Cassim FHI, Cassim MF, Cassim R, Jooste R, Shevy J, Yeats JL, *Contemporary Company Law* 2nd edn (Juta and Company 2011).

Colombo, *Law of Corporate Officers and Directors: Rights, Duties and Liabilities*

> Colombo RJ, *Law of Corporate Officers and Directors: Rights, Duties and Liabilities* 2020-2021 edn (Thomson Reuters 2020).

Davidoff, *Data Breaches: Crisis and Opportunity*

> Davidoff S, *Data Breaches: Crisis and Opportunity* (Boston Addison-Wesley 2020).

Fowler, *Data Breach Preparation and Response: Breaches are Certain, Impact is Not*

> Fowler K, *Data Breach Preparation and Response: Breaches are Certain, Impact is Not* (Cambridge, Ma, Syngress 2016).

Gorecki, *A Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk* Indianapolis

> Gorecki A, *Cyber Breach Response That Actually Works: Organizational Approach to Managing Residual Risk* (Indianapolis John Wiley and Sons 2020).

Neethling and Potgieter, *Law of Delict*

> Neethling J and Potgieter JM, *Law of Delict* 8th edn (LexisNexis SA 2020).

Wilson and Dalziel, *Cyber Security Awareness for CEOs and Management*

> Wilson D and Dalziel H, *Cyber Security Awareness for CEOs and Management* (Waltham, Ma, Syngress, 2016).

Journal Articles

SA

Ahmed 2021 PER / PELJ

Ahmed R, 'The standard of the reasonable person in determining negligence – comparative conclusions' 2021 (24) *Potchefstroom Electronic Review / Potchefstroom Electronic Law Journal* 1–55.

Bekink 2008 SA Merc LJ

Bekink M, 'An historical overview of the director's duty of care and skill: from nineteenth century to the Companies Bill of 2007' 2008 *South African Mercantile Law Journal* 95–116.

Bouwman 2009 SA Merc LJ

Bouwman N, 'An appraisal of the modification of the director's duty of care and skill' 2009 (21) *South African Mercantile Law Journal* 509–534.

Cassidy 2009 SA Merc LJ

Cassidy J, 'Models for reform: the directors' duty of care in a modern commercial world' 2009 (3) *South African Mercantile Law Journal* 373–406.

Cassim 2014 SA Merc LJ

Cassim FC, 'Costs orders, obstacles and barriers to the derivative action under section 165 of the Companies Act 71 of 2008 (Part 1)' 2014 *South African Mercantile Law Journal* 1–23.

Cassim 2011 CILSA

Cassim F, 'Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players' 2011 *The Comparative and International Law Journal of Southern Africa* 123–138.

Chitimira and Ncube 2021 PER / PELJ

Chitimira H and Ncube P, 'The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks' 2021(24) *Potchefstroomse Elektroniese Regsblad/ Potchefstroom Electronic Law Journal* 1–33.

Coetzee 2010 Acta Juridica

Coetzee L, 'A comparative analysis of the derivative litigation proceedings under the Companies Act 61 of 1973 and the Companies Act 71 of 2008: corporate governance and mergers and takeovers: Part II' 2010 *Acta Juridica* 290–305.

Coetzee and Van Tonder 2016 Journal for Judicial Science

Coetzee L and Van Tonder J, 'Advantages and disadvantages of partial codification of directors' duties in the South African Companies Act 71 of 2008' 2016 *Journal for Judicial Science* 1–13.

Du Plessis 2010 Acta Juridica

Du Plessis JJ, 'A comparative analysis of directors' duties of care, skill and diligence in South Africa and Australia' 2010 *Acta Juridica* 263–289.

Esser and Delport 2011 THRHR

Esser IM and Delport P, 'The duty of care, skill and diligence: the King Report and the 2008 Companies Act' 2011 (74) *Journal for Juridical Science* 449–455.

Ezeji CL, Olutola AA and Bello PO 2018 *Acta Criminologica*

Ezeji CL, Olutola AA and Bello PO, 'Cyber-related crime in South Africa: extent and perspectives of state's roleplayers' 2018 *Acta Criminologica: Southern African Journal of Criminology* 93–110.

Farrar 2011 SAcLJ

Farrar JH, 'Directors' Duties of Care: Issue of Classification, Solvency and Business Judgment and the Dangers of Legal Transplants' 2011 *Singapore Academy of Law Journal* 745–761.

Hamadziripi and Chitimira 2021 PER / PELJ

Hamadziripi R and Chitimira H, 'The integration and reliance on technology to enhance the independence and accountability of company directors in South Africa' 2021 (24) *Potchefstroomse Elektroniese Regsblad/ Potchefstroom Electronic Law Journal* 1–32.

Havenga 2000 SA Merc LJ

Havenga M, 'The business judgment rule –should we follow the Australian example?' 2000 *South African Mercantile Law Journal* 25–37.

Jones 2007 SA Merc LJ

Jones E, 'Directors' duties: negligence and the business judgment rule' 2007 *South African Mercantile Law Journal* 326–336.

Kennedy Good and Coetzee 2006 Obiter 1

Kennedy-Good S and Coetzee L, 'The business judgment rule (Part 1)' (2006) *Obiter* 62–74.

Kennedy-Good and Coetzee 2006 Obiter 2

Kennedy-Good S and Coetzee L, 'The business judgment rule (Part 2)' (2006) *Obiter* 277–292.

Lee 2005 Botswana LJ

Lee A, 'Business judgment rule: should South African corporate law follow the King Report's recommendations?' (2005) *Botswana Law Journal* 50–84.

McLennan 1996 SA Merc LJ

McLennan JS, 'Duties of care and skill of company directors and their liability for negligence' 1996 (8) *South African Mercantile Law Journal* 94–102.

Midgley 2000 Acta Juridica

Midgley JR, 'Principles of liability in the modern law of delict: holy cows or horses for courses' 2000 *Acta Juridica* 79–98.

Mongalo 2016 JCCL&P

Mongalo TH, ‘Directors’ standards of conduct under the South African Companies Act and the possible influence of Delaware Law’ 2016 *The Journal of Corporate and Commercial Law & Practice* 1–16.

Mupangavanhu 2017 Stell LR

Mupangavanhu BM, ‘Fiduciary duty and duty of care under Companies Act 2008: does South African law insist on the two duties being kept separate?’ 2017 (1) *Stellenbosch Law Review* 148–163.

Phungula 2016 SA Merc LJ

Phungula S, ‘Lessons to be learned from reckless and fraudulent trading by company: Section 424(1) of the companies act 61 of 1973 and Sections 22 and 77(3)(b) of the Companies Act 71 of 2008’ (2016) *South African Mercantile Law Journal* 28(2) 238–249.

Stevens and De Beer 2016 SA Merc LJ

Stevens R and De Beer P, ‘The duty of care and skill, and reckless trading: remedies in flux?’ (2016) 2 *South African Mercantile Law Journal* 250–284.

Swart and Lombard 2015 THRHR

Swart WJC and Lombard M, ‘Winding up of Companies back to basics *Boschpoort Ondernemings (Pty) Ltd v ABSA Bank Ltd*’ (2015) 78 *Journal for Juridical Science* 356–362.

Theron and Koornhof 2016 ACCC

Theron H and Koornhof P, ‘Bow to the King (IV)? A new era for IT governance in South Africa’ 2016 *Proceedings of the African Cyber Citizenship Conference* 161–173.

Van der Linde 2008 SA Merc LJ

Van der Linde K, ‘The personal liability of directors for corporate fault- an exploration’ (2008) 20 *South African Mercantile Law Journal* 439–461.

Van Tonder 2018 Obiter

Van Tonder JL, ‘A primer on the directors’ oversight function as a standard of directors’ conduct under the Companies Act 71 of 2008’ (2018) *Obiter* 302–316.

Van Tonder 2016 Obiter

Van Tonder JL, ‘An analysis of the directors’ decision-making function through the lens of the business-judgment rule’ (2016) *Obiter* 562–580.

Whitler and Farris 2017 JAR

Whitler KA and Farris PW, ‘The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches’ 2017 (57) *Journal of Advertising Research* 3–9.

US

Ackerman 2019 Wayne St. UJ Bus L

Ackerman B, ‘The fiduciary duties of the board of directors: cybersecurity potential liability and preventative actions’ 2019 *Wayne State University Journal of Business Law 2* 12–32.

Benjamin 2019 GA. St. U. L Rev

Benjamin PE, ‘Cybersecurity oversight liability’ 2019 *Georgia State University Law Review* 663–677.

Furlow 2009 Utah LR

Furlow CW, ‘Good faith, fiduciary duties, and the business judgment rule in Delaware’ 2009 *Utah Law Review* 1061–1095.

Horton 2016 Del J Corp L

Horton BJ, “Modifying fiduciary duties in Delaware: Observing ten years of decisional law” 2016 *40(3) Delaware Journal of Corporate Law* 921–988.

Lafferty, Smith and Wolfe 2011 Penn. St. LR

Lafferty WM, Schmidt LA and Wolfe DJ, ‘A brief introduction to the fiduciary duties of directors under Delaware law’ 2011 *Pennsylvania State Law Review* 116 837–877.

McNeill and Frank 2019 Am. Bankr. LJ

McNeill RS and Frank AG, ‘Waivers and their consequences: an analysis of the limitation of fiduciary duties in Delaware LLC bankruptcies’ 2019 93(4) *American Bankruptcy Law Journal* 649–680.

Mitchell 2018 Loy. L.A.LR

Mitchell E, ‘Caremark’s hidden promise’ 2018 *Loyola of Los Angeles Law Review* 239–290.

Palm and Kearney 1995 Vill LR

Palm CW and Kearney MA, ‘A primer on the basics of directors’ duties in Delaware: the rules of the game (Part 1)’ 1995 *Villanova Law Review* 40 1297–1364.

Sale 2004 Cornell LR

Sale HA, ‘Delaware’s good faith’ 2004 *Cornell Law Review* 456–495.

Internet sources

Acronis, 'The NHS Cyber Attack: How and Why It Happened, and Who Did It' Acronis.com, 2020. Available at www.acronis.com/en-us/articles/nhs-cyber-attack/ (Date of use: 10 March 2021).

Cybok, 'The Cyber Security Body of Knowledge'. Available at https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf (Date of use: 10 March 2021).

Department for Trade and Industry, 'South African Company Law for the 21st Century Guidelines for Corporate Law Reform'. Available at https://www.gov.za/sites/default/files/gcis_document/201409/26493gen1183a.pdf (Date of use: 24 May 2021).

Esser IM and Delport P, 'The South African King IV Report on corporate governance: is the crown shiny enough?'. Available at http://eprints.gla.ac.uk/163223/7/163223.pdf (Date of use: 24 June 2021).

Hosken G, 'Data from huge Experian breach found on the internet' *Sunday Times.* Available at https://www.timeslive.co.za/sunday-times/news/2020-09-13-data-from-huge-experian-breach-found-on-the-internet/ (Date of use: 14 September 2020).

IBM Corporation, 'Cost of a Data Breach Report 2020'. Available at https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (Date of use: 15 September 2020).

Mimecast, 'The State of Email Security 2020'. Available at https://www.mimecast.com/globalassets/cyber-resilience-content/the_state_of_email_security_report_2020.pdf (Date of use: 16 September 2020).

Nieselow T, 'Five massive data breaches affecting South Africans' *Mail & Guardian Online.* Available at https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/ (Date of use: 9 September 2021).

Ngqakamba S, 'Justice department's IT system brought down in ransomware attack' *News24.* Available at https://www.news24.com/news24/southafrica/news/justice-departments-it-system-brought-down-in-ransomware-attack-20210909 (Date of use: 9 September 2021).

Norton, 'What is a security breach?'. Available at https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html (Date of use: 15 September 2020).

SEDA, ‘SMME Quarterly Update 3rd Quarter 2020’. Available at http://www.seda.org.za/Publications/Publications/SMME%20Quarterly%20Sector%20Report%20Q3%202020.pdf (Date of use: 24 March 2021).

Smith D and Harrison J, ‘Experian Exposed to South Africa’s Biggest Ever Data Breach | Lexology’ (*www.lexology.com*, 21 Aug. 2020). Available at www.lexology.com/library/detail.aspx?g=490b5628-9f6b-4e89-93bb-6fe3cf4ae6be#:~:text=On%20Wednesday%2019%20August%202020 (Date of use: 10 March 2021).

Swinhoe D, ‘The 18 Biggest Data Breaches of the 21st Century’ CSO Online (20 December 2018). Available at www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (Date of use: 10 March 2021).

Toyana S, ‘Cybersecurity: South African companies are ripe for hackers’ *Daily Maverick.* Available at https://www.dailymaverick.co.za/article/2021-08-01-cybersecurity-south-african-companies-are-ripe-for-hackers/ (Date of use: 9 September 2021).

Virgin Active South Africa, ‘Cyber Attack’. Available at https://hello.virginactive.co.za/assist/cyber-attack (Date of use: 9 September 2021).

World Economic Forum, ‘The Global Risks Report 2021’ (19 January 2021). Available at http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (Date of use: 10 March 2021).