LEGAL AND ETHICAL CHALLENGES IN CYBERSECURITY GOVERNANCE: A SOUTH AFRICAN PERSPECTIVE ON CORPORATE RESPONSIBILITY AND PROTECTION AGAINST CYBERCRIMES

SUBMITTED TO THE FACULTY OF LAW, UNIVERSITY OF CAPE TOWN, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF LAW WITH SPECIALIASATION IN COMMERCIAL LAW

By

EMERENTIA NTEBOGENG MORAPE

STUDENT NUMBER: MRPEME001

MASTERS IN COMMERCIAL LAW

SUPERVISOR: DR MIKOVHE MAPHIRI

2024

[24 011 words]

DECLARATION

I hereby declare that I have read and understood the regulations governing the submission of this Masters of Law in Commercial Law dissertation, including those relating to length and plagiarism, as contained in the rules of the University of Cape Town, and that this dissertation conforms to those regulations. In conducting this dissertation, ethical principles were diligently upheld in the utilisation of artificial intelligence ("AI") and associated AI tools.

DEDICATION

The highest praise and thanks go to my Lord and Saviour, Jesus Christ, who carried me through all thus far in my life. I give all that I have to you, including the energy and time that went into writing and finishing this dissertation.

This dissertation is dedicated to my younger brother, Neo Morape, who has been my biggest cheerleader in everything that I do! As you take John 13:7 (your favourite scripture) with you, I hope you know that you can be better and do bigger things than what you see in this world, and God will bless your dreams. You rock kid!

This dissertation is also dedicated to my mentor and the coolest CIO, Ashley Singh. I would like to express my heartfelt gratitude for the immense inspiration you've provided in my Masters journey. Conversations with you truly ignited my own interest in Cybersecurity and Innovation, leading me to embark on this journey of writing a master's dissertation in this domain. Thank you for igniting my passion and guiding me towards this fulfilling path. Your mentorship has made a profound impact on my academic and personal growth, and I am grateful for your guidance and always believing in me.

To my parents, Akanyang and Kehilwe Morape, words can't express how thankful I am for everything you've done for me. Your support has been crucial in my academic achievements and personal growth. Thank you for your endless support, patience, and love. You have been my rock throughout my life and academic journey, and I am forever grateful.

To my youngest siblings, Junior and Didimalang, I hope I make you proud as a sister and that I will be able to witness all the great things that you will grow up to do.

A special thanks and shout out to Valentino Collison, who has been an incredible relentless cheerleader cheering me on and celebrating every small achievement, professionally and academically. Thank you for having a kind heart and always giving great advice! Another shutout to Cheslyn, an amazing UWC LLD candidate, thanks for being a sounding board and reviewing my work. Your help made a big difference.

To my friends, words can't even begin to describe how grateful I am for all your love and support through this journey. All the love and encouragement are greatly received and appreciated – Molefi, Yamkela, Azahlia, Karabelo, Martin, Ruwayda, Bofelo, Lorenzo, Neo, Sylvio, Mbali, Servane, Kelly, Boitumelo, Andrew and Ntshepi – I love and appreciate you all so much!

ACKNOWLDEGEMENT

I would like to acknowledge and appreciate my supervisor, Dr Mikovhe Maphiri, for her guidance and support with this dissertation and for believing in my research and writing abilities. You have become a role model for me and made me believe that I could achieve anything and have success in life and in academics. Your expertise, patience, and encouragement have been instrumental in helping me navigate the challenges and complexities of the research process.

Your insightful feedback and constructive criticism have not only strengthened my dissertation but have also enhanced my skills as a researcher. I am truly grateful for the time and dedication you have invested in me, ensuring that I produce work of the highest quality. Your mentorship has been invaluable to me, and I am immensely thankful for your unwavering support every step of the way. It has been an honour and a privilege to work under your guidance, and I am proud of the work that we have accomplished together.

I would like to send love, acknowledgement and appreciation to Dr Jo-Mari Visser, who was my lecturer and supervisor for my LLB mini-dissertation at the University of the Free State. Thank you for still being a constant source of support and encouragement. Whenever I reflect on my undergraduate experience, I am grateful for the lessons I have learned and the skills I have acquired, many of which I owe to your guidance. Your passion for teaching and your commitment to excellence have inspired me to strive for the highest standards in all that I do. Thank you once again for your unwavering support and encouragement. I am proud to have had the opportunity to learn from you and to be able to carry those lessons with me on every journey that I embark on.

A special thanks to our senior faculty librarian, Ms Anthea Paulsen, for assisting me with my dissertation referencing, ensuring that I don’t plagiarise. Your help and guidance are truly appreciated.

My academic journey took a village to get thus far. I would like to show appreciation to my grade 1 teacher, Mam Jammer and high school teacher, Mam Mynhardt. Having the teachers who supported and encouraged me from my early academic development share such academic milestones with me has been heart-warming, I hope that I can continue to make you proud. My heartfelt gratitude to the JB Marks Education Trust Fund and the people in the office for their financial support from the beginning of my academic career in LLB to my LLM. Mme Refilwe, Mam Judy, Mme Nozipho, Buti Nkululeko and Mme Vonani, thank you for always taking my calls and emails and assisting me from day one!

TABLE OF CONTENTS

ACRONYMS 8

ABSTRACT 9

CHAPTER ONE: INTRODUCTION 10

1. BACKGROUND OF CYBERSECURITY 10

1.1 PURPOSE OF RESEARCH 15

1.2 RESEARCH QUESTIONS 15

1.3 DELINEATIONS AND LIMITATIONS 16

1.4 RESEARCH OBJECTIVE 17

1.5 RESEARCH METHODOLOGY 18

1.6 STRUCTURE OF DISSERTATION 18

2.1 AN OVERVIEW OF CORPORATE GOVERNANCE IN CYBERSECURITY 19

2.2 CORPORATE GOVERNANCE WITHIN THE FRAMEWORK OF SOUTH AFRICAN LAW: AN OVERVIEW 21

2.2.1 IILUSTRATIONS OF EFFECTIVE CORPORATE GOVERNANCE PRACTICES 25

2.2.2 IILUSTRATIONS OF INEFFECTIVE CORPORATE GOVERNANCE PRACTICES 28

2.3 A SYNOPSIS OF THE LEGISLATION AND FRAMEWORK THAT GOVERN CYBERSECURITY 30

2.3.1 ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 of 2002 31

2.3.2 CYBERCRIMES ACT 19 of 2020 34

2.3.3 PROTECTION OF PERSONAL INFORMATION ACT 14 of 2013 36

2.3.4 COMPANIES ACT 71 OF 2008 AND KING IV CODES ON CORPORATE GOVERNANCE 39

2.4 DO THESE LEGISLATION PROVIDE ENOUGH SECURITY AND LEGAL PROTECTION FOR COMPANIES? 41

2.5 CONCLUSION 43

CHAPTER THREE: CYBERCRIMES AND CYBERATTACKS IN CORPORATE GOVERNANCE 44

3.1 A PRECIS OF CYBERSECURITY 44

3.2 THE DIFFERENT CYBERCRIMES, CYBERATTACKS AND CYBERETHICS 45

3.2.1 SOME OF THE DIFFERENT CYBERCRIMES AND CYBERATTACKS 45

3.2.2 LEGAL ETHICS IN CYBERSECURITY: AN OVERVIEW 50

3.3 HOW CYBERCRIMES AND CYBERATTACKS ARE COMBATTED 51

3.4 FOSTERING A CULTURE OF CYBERSECURITY AWARENESS AND TRAINING WITH DIFFERENT STAKEHOLDERS 53

3.4.1 HOW A CULTURE OF CYBERSECURITY AWARENESS CAN BE FORSTERED 53

3.5 CONCLUSION 55

CHAPTER FOUR: LEGAL AND ETHICAL IMPLICATIONS OF CYBERSECURITY AND PRIVACY LAWS 57

4.1 INTRODUCTION 57

4.2 LEGAL IMPLICATIONS OF CYBERSECURITY AND PRIVACY LAWS 58

4.3 ETHICAL IMPLICATIONS OF CYBERSECURITY AND PRIVACY LAWS 60

4.4 FRAMEWORKS AND PROTOCOLS FOR CYBERATTACKS AND DATA BREACHES 63

4.4.1 PROTOCOLS FOR REPORTING IN THE EVENT OF CYBERATTACKS AND DATA BREACHES 64

4.4.2 PROTOCOLS FOR RESPONDING IN THE EVENT OF CYBERATTACKS AND DATA BREACHES 65

4.4.3 PROTOCOLS FOR RECOVERING IN THE EVENT OF CYBERATTACKS AND DATA BREACHES 66

4.5 A DISCUSSION OF THE IMPLICATIONS OF DATA BREACHES ON COMPANIES AND STAKEHOLDERS 68

4.6 CONCLUSION 71

CHAPTER FIVE: RECOMMENDATIONS AND CONCLUSION 72

5.1 SUMMARY OF FINDINGS 72

5.2 RESEARCH QUESTIONS ANSWERED 73

5.3 CONCLUSION AND RECOMMENDATIONS 73

BIBLIOGRAPHY 75

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial Intelligence
BAS	Breach and Attack Simulations
BEC	Business Email Compromise
BBBEE	Broad-based Black Economic Empowerment
C4IR Rwanda	Centre for the Fourth Industrial Revolution
CAIR	Centre for Artificial Intelligence Research
CSIR	Centre for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
ECTA	Electronic Communication and Transactions Act 25 of 2002
ESG	Environmental, Social and Governance practices
IP	Internet Protocol
ISIMC	Information Security Incident Management Capability
IT	Information Technology
JSE	Johannesburg Stock Exchange
MIS	Management Information System
NCPF	National Cybersecurity Policy Framework
NCAIR	National Centre for Artificial Intelligence and Robotics
NDEPS	National Digital Economy Policy and Strategy
NTIDA	National Information Technology Development Agency
POPIA	Protection of Personal Information Act 4 of 2013

ABSTRACT

In the current digital era, cybersecurity has become a vital aspect of corporate governance, presenting challenging moral and legal issues for businesses all over the world. This dissertation examines the complex relationship between legal frameworks, ethical deliberations, and organisational duties as they relate to cybersecurity within the context of corporate governance. It clarifies the dynamic nature of cybersecurity rules and regulations by looking at different case law and journal papers, highlighting the necessity of taking preventative action to reduce cyber risks and guarantee compliance. This paper also explores the many cybercrimes as defined by the Cybercrimes Act 19 of 2020, the various laws governing cybersecurity in South Africa, as well as the ethical aspects of cybersecurity, and how privacy and data protection are addressed. It highlights how crucial it is for businesses to have a culture of ethical consciousness and responsibility in order to protect sensitive data and maintain stakeholder trust. This dissertation offers insightful guidance and useful suggestions for managing the complicated realm of cybersecurity in corporate governance, strengthening organisational resilience and integrity against constantly changing cyberthreats, by means of an extensive examination of legal and ethical implications.

CHAPTER ONE: INTRODUCTION

1. BACKGROUND OF CYBERSECURITY

One of the most important areas of information technology is cybersecurity.[1] Contrary to what many people believe, the field of cyber security has existed for quite some time. It dates back to the 1980s when a "worm program," (also known as "The Morris Worm") that was developed by Robert Tappan Morris, spread across the internet and caused significant disruptions to computer networks and systems.[2] This worm was notorious for its elusive nature, making it difficult to track down and remove.[3] The inventor of the "worm program" was then prosecuted in the *United States v Morris*[4] case and it contributed to the development of information technology crime laws and computer security procedures.[5]

Creating a secure internet environment is a difficult task that calls for a methodical, all-encompassing approach to recognise and reduce possible security vulnerabilities.[6] In regard to this, cybersecurity research factors are essential since they offer the basis for creating and putting into practice security solutions that can handle new threats.[7] Cyberattacks[8] and Cybercrime involved the digital technology as well as private data processing such as "data breaches, identity theft and cyber fraud".[9] Cybercrime is defined as

> "any criminal activity that involves a computer and includes crimes which previously existed before computers but now committed in a cyber environment such as fraud or child

---

1 Kala refers to Cybersecurity as "the ability to protect a user's assets and the environment in which they operate from intrusion by an outside party" in Emiles Mbungu Kala "The Impact of Cyber Security on Business: How to Protect Your Business" (2023) 13(2) *Open Journal of Safety Science and Technology* 51.

2 Eugene Spafford "The Internet Worm Program: An Analysis" (1988) *Purdue Technical Report CSD-1R-823* 23.

3 Ibid footnote 2.

4 *United States v Morris* 728 F. Supp. 95 (1990).

5 Ibid footnote 4.

6 Muhammad Safitra, Muharman Lubis and Hanif Fakhrurroja "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity" (2023) 15 *Sustainability* 18.

7 Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, *et al* "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review" (2023) 23 (4117) *Sensors* 1.

8 Cyberattacks are defined as "malicious attempts to steal, expose or destroy data through unauthorized access to a computer system. The breached system can then be used to launch further attacks." See Mimecast "Cyberattack" available at https://www.mimecast.com/content/cyber-attack/, accessed on 06 April 2024

9 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 300.

pornography and crimes which became possible because of the computer such as hacking, cracking and sniffing."[10]

Cybercrime has become one of the fastest growing criminal sectors globally, a trend that became evident in 2020 when the COVID-19 pandemic brought an increase in cyber-attacks as the epidemic gave hackers new targets to take advantage of.[11] However, since pandemic the South African government pledged to use technology to its greatest advantage for its people and established foundations for laws and supporting policies to help regulate behaviours occurring in cyberspace.[12] A detailed discussion of these laws will take place in chapter two.

Cyber-related crimes are becoming more frequent worldwide, and the widespread occurrence of cyber incidents worldwide adds to the escalating worries surrounding cybersecurity.[13] The World Economic Forum found that hackers and organised cybercrime syndicates represent significant external risks for companies, in 31% of external fraud cases, hackers were identified as the perpetrators, while organised crime groups were responsible for 28% of cases, and these figures notably increased when compared to 2020.[14]

The global Cybercrime statistics conducted by AAG IT Services[15] found thatin 2022, the United Kingdom and the United States of America witnessed notable trends in cybercrime. The United Kingdom experienced a significant surge in victims, reaching 4783 per million internet users, up by 40% from 2020, while the United States of America saw 1494 victims per million internet users, representing a 13% decrease from the previous year. North America had a high breach rate, affecting 1 in 2 internet users in 2021. Both the United Kingdom and the United States of America had considerably higher cybercrime victim rates compared to other countries, with the USA observing 759% more victims than Canada, the next-highest country. The Netherlands noted a 50% rise in victims in 2022, while Greece saw a notable decrease of 75% compared to 2020. Globally, there were, on average, 97 data breach victims per hour in 2021. In the Asia-Pacific

---

10 Sizwe Snail "Cybercrime in South Africa – Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law & Technology* 2.

11 Heloise Pieterse "The Cyber Threat Landscape in South Africa: A 10-Year Review" (2021) 28 *The African Journal of Information and Communication* 2.

12 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 300.

13 Ibid footnote 11 at 1

14 World Economic Forum "Nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat. What can they do about it?", available at *https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/*, accessed on 06 April 2024.

15 An award-winning IT Services company in the United Kingdom.

region, cybercrime surged by 168% between May 2020 and 2021, with Japan experiencing a 40% increase in cyber-attacks in May 2021 compared to earlier months. Notably, between Quarter 2 and Quarter 3 of 2022, China, Japan, and South Korea saw significant rises in data breaches, with increases of 4852%, 1423%, and 1007% respectively, leading to substantial numbers of breached accounts in each country.[16]

Cyber-attacks become more frequent and more severe as technological innovation advances and people become more dependent on it.[17] South Africa is no different. In *Buchler v Minister of SAPS N.O. and Others*[18], the internet café where Buchler worked was raided by the Police and Hawks ("the authorities") on suspicion that Buchler was utilising the materials to carry out unlawful internet gambling practices. The authorities had warrants to search and take possession of materials to investigate the possible unlawful gambling practices. The court determined that the warrants, upon which the authorities had relied, were void due to their vagueness and were directed by the court to give Buchler back all items that had been taken.[19] This case can lead to companies asking whether or not they are protected by the law from cyber risks and reputational damages from flawed investigations and accusations.

Cybercrimes are posing a serious threat to South African companies,[20] and the effects are dire as cyberattacks are increasing frequently, which is a serious issue for the corporate community.[21] These effects include a data leak incident that took place in May 2020, where the confidential information of employers that were in the Unemployment Insurance Fund ("UIF") database was leaked[22], and shortly thereafter in 2021, a privacy breach affecting the Department of Justice and Constitutional Development's Information Technology ("IT") system was verified.[23]

---

16 This a study conducted by Charles Griffiths from AAG IT Services, see Charles Griffiths "The Latest 2024 Cyber Crime Statistics (updated March 2024)" available at *https://aag-it.com/the-latest-cyber-crime-statistics/*, accessed on 04 April 2024.

17 Heloise Pieterse "The Cyber Threat Landscape in South Africa: A 10-Year Review" (2021) 28 *The African Journal of Information and Communication* 1.

18 *Buchler v Minister of SAPS N.O. and Others* (6310/2022) [2023] ZAFSHC 1 (5 January 2023).

19 The court referred to the *Goqwana v Minister of Safety NO and Others* 2016 (1) SACR 384 (SCA) case in this regard.

20 Some cyber incidents identified to have taken place from 2010 to 2020 in South African companies are "data exposure, denial of services, defacement, and system penetration". See Brett van Niekerk "An analysis of Cyber-Incidents in South Africa" (2017) 20 *The African Journal of Information and Communication* 117-121.

21 The words corporate and companies will be used interchangeably throughout the paper.

22 Ibid footnote 17 at 2.

23 Ibid footnote 17 at 2.

Ransomware was the cause of the intrusion, rendering all departmental systems inaccessible to both public and internal users due to encryption.[24]

The risks and consequences of a breach of cybersecurity or cyber-threat[25] can be significant and varied, including:

- Present serious dangers to businesses, such as financial losses, privacy violations, and company interruption.[26]
- Reputation Damage: There is little research on the impact of data breaches on a company's reputation or the extent of such effects, however data breaches can severely harm a company's reputation and erode trust among customers, clients, and partners.[27] Negative media and damage to a company's reputation can have long-lasting consequences, such as the loss of collaborators, clients, and business opportunities.[28]
- Regulatory Penalties: violations of data protection, industry rules, contractual duties, and privacy regulations can result in significant penalties, depending on the jurisdiction.[29]
- Loss of Trade Secrets: In cases of corporate espionage, critical trade secrets that are key to innovation and intellectual property may be exposed or stolen.[30]
- Disruption of operations: Cyber hacking has the ability to compromise important business and governmental operations, resulting in lost time, lower output, and inefficiencies in service delivery. Ransomware attacks, for example, has the ability to steal data and render

---

24 Heloise Pieterse "The Cyber Threat Landscape in South Africa: A 10-Year Review" (2021) 28 *The African Journal of Information and Communication* 3.

25 Cyber threats are "any hostile acts that are carried out by individuals or groups making use of technology to inflict harm to individuals, businesses, or even nations. These dangers can manifest themselves in a wide variety of ways, including cyberattacks, data breaches, hacking, identity theft, ransomware, phishing, and many more". See Emiles Mbungu Kala "The Impact of Cyber Security on Business: How to Protect Your Business" (2023) 13(2) *Open Journal of Safety Science and Technology* 58.

26 Frank Cremer, Barry Sheehan, Michael Fortmann, *et al* "Cyber risk and cybersecurity: a systematic review of data availability" (2022) 47 *The Geneva Papers on Risk and Insurance – Issues and Practice* 699.

27 Christo Makridis "Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018" (2021) *Journal of Cybersecurity* 6.

28 Emiles Mbungu Kala "The Impact of Cyber Security on Business: How to Protect Your Business" (2023) 13(2) *Open Journal of Safety Science and Technology* 56.

29 Section 107 of the Protection of Personal Information Act 4 of 2013.

30 This is discussed in the *Rockwell Graphic Systems, Inc. v DEV Industries, Inc*., 925 F.2d 174 (1991) case where it stated that "trade secret protection is an important part of intellectual property, a form of property that is of growing importance to the competitiveness of American industry" and that "[t]he future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends in no small part on the protection of intellectual property".

> systems or networks inoperable, which can cause monetary harm and commercial interruptions.[31]

This creates a need for companies to be cyber resilient and advance the safe use of technology and the techniques by which ever-more complex attacks are prevented from damaging organisational assets with clear ethical frameworks.[32] Organisations can balance concerns about security, confidentiality, and accountability as they relate to data by using the guiding principles provided by cybersecurity ethics.[33] Laws[34] governing cybersecurity can be helpful in this sense, especially when combined with corporate governance principles.[35] Essentially, regulatory and policy structures will need to change in order to more effectively combat cybercrime and attacks, malicious cyber activities, the use of the internet for terrorist purposes, and the propagation of extremism that is violent. These changes must also be made in order to better respect and enforce international human rights standards.[36]

There is a lot of innovation happening around the world within companies in regards to cybersecurity, ethics and law, which has led to a lot of efficiencies for companies and individuals, but it also significantly increased vulnerability.[37] While modern advancements like artificial intelligence ("AI")[38] and digitisation can produce enormous benefits in practically every field, when applied improperly, they can also have detrimental effects.[39] Therefore, businesses need to take precautions to stop hackers from taking over their networks and stealing their data.

---

31 Emiles Mbungu Kala "The Impact of Cyber Security on Business: How to Protect Your Business" (2023) 13(2) *Open Journal of Safety Science and Technology* 56.

32 Muhammad Safitra, Muharman Lubis and Hanif Fakhrurroja "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity" (2023) 15 *Sustainability* 4.

33 Cybersecurity ethics (also known as "cyber ethics") are "the study and analysis of moral principles and conundrums as well as a look at the laws, norms, and regulations that control behaviour in cyberspace and the cyber realm." See Aderinola Dunmade, Adeyinka Tella and Uloma Onuoha "Cyberethics awareness and implications on Library and Information Science educators in selected Universities in South-West Nigeria" (2023) 89(1) *South African Journal of Libraries and Information Science* 2.

34 See *inter alia* the Cybercrimes Act 19 of 2020, Protection of Personal Information Act 4 of 2013, Electronic Communications and Transactions Act 25 of 2002, and Companies Act 71 of 2008.

35 These principles will be discussed in chapter 2 below.

36 See Alok Mishra, Yehia Alzoubi, Memoona Anwar, *et al* "Attributes impacting cybersecurity policy development: An evidence from seven nations" (2022) *Computers & Security* 2-4.

37 Examples of the innovation include "Artificial Intelligence, Cloud computing, Autonomous vehicles, and Big Data and Machine Learning." See Lubna Dhirani, Noorain Mukhtiar, Bhawani Chowdhry, *et al* "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review" (2023) 23(3) *Sensors* 1

38 Artificial Intelligence is defined as "a system's ability to correctly interpret external data, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation." See Michael Haenlein and Andreas Kaplan "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence" (2019) 61(4) *California Management Review* 1.

39 Lubna Dhirani, Noorain Mukhtiar, Bhawani Chowdhry, *et al* "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review" (2023) 23(3) *Sensors* 1-3.

In order to safeguard their organisations against security breaches and cyberattacks, South African companies must ensure that their IT and governance departments, with the assistance of security experts, comply with South Africa's cybersecurity laws and ethical standards.

1.1 PURPOSE OF RESEARCH

The purpose of this dissertation is to investigate the cybersecurity laws in South Africa, the protection they provide for companies, and the ethical challenges associated with adopting cybersecurity laws in corporate governance. This dissertation will analyse the complexities of compliance, data protection laws, and potential conflicts between legal requirements and cybersecurity measures. The South African government has put into effect a number of legislation that address cybercrime, governs cybersecurity in the country, and the substantive legal requirements of the Budapest Convention,[40] such as the Cybercrimes Act 19 of 2020, Protection of Personal Information Act 4 of 2013, Electronic Communications and Transactions Act 25 of 2002, and Companies Act 71 of 2008 (as some of the main legislation that governs corporate governance), the King IV report on Corporate Governance in South Africa,[41] case law, journals and technology regulatory frameworks[42] which will also be analysed through this dissertation and will be used to determine how companies combat cyberattacks and cybercrimes.

Corporate governance plays a role of ensuring that the company has cybersecurity frameworks that align with privacy laws and are risk-based in order to combat security-related threats and manage these risks in accordance with the organisation's appetite for cyber-risk.

1.2 RESEARCH QUESTIONS

The main research question to be addressed is:

What legislation governs cybersecurity in South Africa and does the legislation provide enough legal protection for companies against cybercrimes and security breaches?

---

40 Council of Europe "Convention on Cybercrime" available at *https://www.coe.int/en/web/cybercrime/the-budapest-convention*, accessed on 30 November 2023.

41 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

42 Such as frameworks and methods for handling cyberattacks and data breaches, data protection, cybercrime mitigation, and incident response. This will be discussed in chapters 3 and 4 below.

The secondary research questions are:

a) How do companies ensure alignment between their cybersecurity frameworks and privacy laws?

b) How do they cultivate awareness of cybersecurity among all stakeholders?

1.3 DELINEATIONS AND LIMITATIONS

This dissertation provides a comprehensive overview of the legal and ethical challenges in cybersecurity governance, focusing on corporate responsibility and protection against cybercrimes within the South African context. It underscores the critical importance of cybersecurity in the digital age and emphasises the challenging moral and legal dilemmas faced by businesses. However, it is essential to acknowledge some limitations within this discourse.

The scope of this dissertation primarily focuses on cybersecurity within the context of corporate structures, thus limiting the exploration of cybersecurity issues in other sectors or contexts, such as healthcare and education. Additionally, the analysis predominantly centres on South African legislation and corporate governance frameworks, specifically the Cybercrimes Act 19 of 2020 and Protection of Personal Information Act 4 of 2013, which may limit the applicability of the findings to jurisdictions with different legal landscapes. Moreover, the dynamic nature of cybersecurity regulations and ethical standards necessitates a constant reassessment of the findings presented in this dissertation, as new laws, regulations, and ethical frameworks emerge.

Furthermore, while efforts have been made to provide practical guidance and suggestions for managing cybersecurity risks in corporate governance, this dissertation primarily emphasises preventative measures and ethical considerations, with less emphasis on post-incident response strategies. As cybersecurity threats continue to evolve, a comprehensive approach that also includes robust incident management is crucial, and this aspect could be expanded in future research. Despite these limitations, this dissertation aims to contribute to the ongoing discourse surrounding cybersecurity governance, particularly in relation to legal compliance and ethical responsibilities in the face of increasing cyber threats.

1.4 RESEARCH OBJECTIVE

In the field of technology, there is a need for professionals to understand and implement ethical principles. Ethics itself could be understood as a code or moral way by which a person lives and works. However, in the field of information technology and cybersecurity research, there is a possibility that even the technically most appropriate solution may not be compatible with the relevant ethical principles. Experts must implement basic ethical principles in their technical products in order not to cause harm or negative effects to their users.[43]

The vast majority of the challenges faced by these professionals include having appropriate measures to take to ensure compliance with ethical principles. Challenges such as maintaining user privacy, accuracy, accessibility, reporting and handling of random results, testing the technological product, mitigating prejudice, etc. can have different negative impacts on customer service if not handled properly.[44]

Emerging technologies face ethical challenges and governance in managing these technologies that have changed over time,[45] some of these challenges include data privacy,[46] AI risks and ethical concerns, creating sustainable settings, health effects of technology use, infodemic concerns, and the use of data as a weapon.[47]

Corporate governance has become increasingly popular in companies in recent years, and its significance has been emphasised globally.[48] It is widely defined as "a multiple term which means control, leadership, individualism and business management in the area of corporations and economic systems".[49]

---

43 Denitsa Kozhuharova, Atanas Kirov and Zhanin Al-Shargabi "Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?" (2022) *Cybersecurity of Digital Service Chains* 202.

44 Denitsa Kozhuharova, Atanas Kirov and Zhanin Al-Shargabi "Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?" (2022) *Cybersecurity of Digital Service Chains* 214.

45 Lan Xue and Zhenjing Pang "Ethical governance of artificial intelligence: An integrated analytical framework" (2022) 1 *Journal of Digital Economy* 44.

46 Data privacy refer to "the protection of personal information and data from unauthorised access, use, disclosure, disruption, modification, or destruction." See Kamshad Mohsin "Data Privacy and Cybersecurity" (2022) *SSRN* 1.

47 Lubna Dhurani, Noorain Mukhtiar, Bhawani Chowdhry *et al* "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review" (2023) 23(3) *Sensors* 1-3.

48 Manuel Alfonso Garzón Castrillón "The concept of corporate governance" (2021) 25(2) *Revista Científica "Visión de Futuro"* 178.

49 Georgina Broni and John Velentzas "Corporate governance, control and individualism as a definition of

The governance paradigm has gradually shifted from scientific rationality to social rationality and higher ethical morality, and the trend to seek higher levels of ethics and morality provides a rich theoretical foundation for the ethical governance of AI.[50]

1.5 RESEARCH METHODOLOGY

In order to properly investigate the different legislation that govern cyber security in South Africa and the legal and ethical challenges associated with adopting these cybersecurity laws in corporate governance, this dissertation will follow a doctrinal research approach by way of a textual analysis and using primary and secondary sources of law. This approach will be used to analyse the legislation that governs cybersecurity in South Africa and ethical challenges that companies face when adopting them.

1.6 STRUCTURE OF DISSERTATION

Chapter one is an introductory chapter to the research topic. Thereafter, chapter two will evaluate the different legislation that govern cybersecurity in corporate governance and whether they provide enough legal protection for companies against cybercrimes and security breaches.

Chapter three will discussion the different kinds of cybercrimes and cyberattacks that companies struggle with, and how the legislation plays a role in combatting them. It will also look at how companies can foster a culture of cybersecurity awareness and with its different stakeholders.

Chapter four will discuss the legal and ethical challenges that are associated with adopting cybersecurity and privacy laws that help companies combat cybercrimes and security breaches. It will also look at the different frameworks within corporate governance on the protocols for reporting, responding and recovering in the event of a cyberattacks.

Thereafter, chapter five provides the conclusion of the research dissertation, whether innovation plays a role in helping companies combat cybercrimes, recommendations, what other African countries can learn from South Africa on how to combat cybercrimes through legislation and frameworks that govern Cybersecurity, and concluding remarks.

---

[50] business success. The idea of a "post - heroic" leadership" (2012) 1 *Procedia Economics and Finance* 61. Lan Xue and Zhenjing Pang "Ethical governance of artificial intelligence: An integrated analytical framework" (2022) 1 *Journal of Digital Economy* 44.

CHAPTER TWO: CORPORATE GOVERNANCE IN CYBERSECURITY

2.1 AN OVERVIEW OF CORPORATE GOVERNANCE IN CYBERSECURITY

This chapter focuses on the evaluation and discussion of the various laws governing cybersecurity in corporate governance, and then on their adequacy in shielding businesses from cybercrimes and security breaches. As mentioned above, corporate governance can be defined as "a multiple term which means control, leadership, individualism and business management in the area of corporations and economic systems",[51] and seeing how its importance has significantly increased in the last two decades, the changes in the governance of companies has shown that authorities view governance as a critical component for achieving reliable reports on finances.[52]

Cybersecurity is an important issue for businesses given the demand for universal internet access, the growing popularity of social networks, the rising reliance on digital government services, and the widening range of threats from foreign powers, terrorists, and criminals.[53]

The impacts of the increase of cybercrimes also affect South Africa as the nation's rapid technological advancements are expanding the cyber domain's attack field.[54] Phishing, malware, spam emails and ransomware[55] are some of the biggest cyberattacks that the financial services industry in South Africa are faced with amid COVID-19.[56] Because there has been a lot of focus regarding the governance of cybersecurity in recent years, the government implemented the National Cybersecurity Policy Framework ("NCPF")[57] in 2015 in order to establish a secure, dependable, and trustworthy cyber environment that safeguards critical information infrastructure while promoting shared human values and a deeper understanding of cybersecurity.[58] This supports national security objectives and economic growth, fostering an information society that

---

51 Georgina Broni and John Velentzas "Corporate governance, control and individualism as a definition of business success. The idea of a "post - heroic" leadership" (2012) 1 *Procedia Economics and Finance* 61.

52 Nabeelah Daniels and Anna-Retha Smit "Corporate governance and the value relevance of accounting information: Empirical evidence from South Africa" (2023) 25 *Southern African Journal of Accountability and Auditing Research* 21.

53 Ewan Sutherland "Governance of Cybersecurity – the case of South Africa" (2017) 20 *The African Journal of Information and Communication* 83.

54 Heloise Pieterse "The Cyber Threat Landscape in South Africa: A 10-Year Review" (2021) 28 *The African Journal of Information and Communication* 1.

55 These are defined in chapter 3 below.

56 Joel Chigada and Rujeko Madzinga "Cyberattacks and threats during COVID-19: A systematic literature Review" (2021) 23(1) *South African Journal of Information Management* 4.

57 State Security Agency "National Cybersecurity Policy Framework", available at *https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf*, accessed on 07 April 2024.

58 Ibid footnote 57.

upholds the fundamental rights of all South African citizens, including "privacy, security, dignity, access to information, communication, and freedom of expression".[59] This effort was supported by a National Cybersecurity Implementation Plan that was developed by the Justice, Crime and Security Cluster ("JCPS") in collaboration with relevant stakeholders.

The government also created the Information Regulator[60] in order to ensure data privacy and protection, and the coordination of cybersecurity activities[61] through the enactment of the Protection of Personal Information Act ("POPIA")[62] and the Cybercrimes Act[63] that was aimed to support the law enforcement organisations and offer direct services to the general public and businesses.[64]

The South African government has come under fire for its service delivery shortcomings, among which cybersecurity is one even though it is not generally acknowledged.[65] These challenges stem from delays, poor risk assessments, a lack of transparency, and poor coordination between the government, businesses, and society.[66] Businesses often face legal liability for losing customer data, which can result in significant damage to their brand reputation and a decline in customer loyalty. Some businesses are resistant to disclose data breaches as it might lead to financial loss despite it being a legal obligation under the different legislation.[67]

This has increased the need for companies to have good corporate governance in order to protect it from cyberattacks and maintain its reputation, because bad corporate governance can cause companies to collapse and frequently result in scandals or loss of operations and profits, while

---

59 State Security Agency "National Cybersecurity Policy Framework", available at *https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf,* accessed on 07 April 2024.

60 More information about the Information Regulator is available at *https://registrations.inforegulator.org.za/landing*, accessed on 07 April 2024.

61 Ewan Sutherland "Governance of Cybersecurity – the case of South Africa" (2017) 20 *The African Journal of Information and Communication* 84.

62 Protection of Personal Information Act 4 of 2013.

63 Cybercrimes Act 19 of 2020.

64 Ibid footnote 61 at 90.

65 Ibid footnote 61 at 101.

66 Ibid footnote 61 at 101.

67 Ibid footnote 61 at 87.

good corporate governance minimises conflicts of interest and enhance the company's financial performance by boosting its value and delivering higher returns on investment to shareholders.

Moreover, the King IV report on corporate governance in South Africa[68] stated that

> "technology governance and security are now pressing concerns because technology is no longer just an enabler, but is also a part of the corporate DNA as the root of several future opportunities and potential disruptions for an organisation, which is a great demonstration of how opportunity and risks are becoming more and more synonymous".[69]

2.2 CORPORATE GOVERNANCE WITHIN THE FRAMEWORK OF SOUTH AFRICAN LAW: AN OVERVIEW

Corporate governance in South Africa is shaped by a collection of principles and regulations designed to promote transparency, accountability, and fairness in the management and control of companies while tackling obstacles and progressing toward sustainable and accountable business practices.[70] It is mainly governed by the Companies Act[71], King IV Codes on Corporate Governance for South Africa ("King Codes"),[72] and the Johannesburg Stock Exchange ("JSE").[73] Furthermore, Some sectors in South Africa are subject to additional governance regulations and supervision from industry-specific regulatory bodies. For instance, the financial services industry falls under the oversight of the South African Reserve Bank ("SARB")[74] and the Financial Sector Conduct Authority ("FSCA"),[75] each imposing their own governance standards on financial institutions.

---

68 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

69 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

70 PwC South Africa "King IV – Steering point", available at *https://www.pwc.co.za/en/publications/king4.html*, accessed on 24 April 2024.

71 71 of 2008.

72 Ibid footnote 68.

73 The JSE corporate governance framework is available at *https://group.jse.co.za/governance/corporate-governance-framework*, accessed on 25 April 2025.

74 The SARB governance structure is available at *https://www.resbank.co.za/en/home/what-we-do/Prudentialregulation/governance-structures*, accessed on 25 April 2024.

75 The FSCA regulatory strategy is available at *https://www.fsca.co.za/Documents/FSCA_Strategy_2018.pdf*, Accessed on 25 April 2024.

The 2008 Companies Act[76] serves as the main regulatory framework governing corporate governance in South Africa. The Act outlines the legal guidelines for company governance within South Africa, as well as the duties and responsibilities of directors, including the promotion of the best interests of the company and the exercise of reasonable care, skill, and diligence.[77] The King Codes which was introduced on 1 November 2016, although not legally binding, offers principles and guidance for achieving efficient corporate governance and it emphasises ethical leadership, effective control, good performance, legitimacy, and sustainability.[78] The JSE plays a significant role in enhancing corporate governance practices and protecting the interests of stakeholders in South Africa's capital markets by obliging their listed companies to disclose the level of adherence to the King Codes guidelines in their annual reports.[79] These include provisions relating to the "composition of the board, risk management, remuneration and sustainability".[80]

Important components of corporate governance in South Africa are corporate accountability, board composition, managerial control, and corporate reporting and disclosure. Several legal and regulatory frameworks, industry regulations, and best practices address these issues.

In corporate accountability, section 76 of the Companies Act[81] outlines the fiduciary duties of directors, emphasising that it requires them to act honestly, with good faith, and in a way that they reasonably think is in the best interests and to the benefit of their companies,[82] and it was later confirmed by the court in *Cyberscene Ltd v i-Kiosk Internet and Information (Pty) Ltd*[83] that a fiduciary duty exists between a company and its directors. Section 76(3) goes beyond the common law duty of directors and addresses the quality of conduct expected from them.[84]

With regards to board structure, section 66 of the Companies Act[85] provides guidelines for board composition, such as the designation of non-executive directors who are independent and the division of the chairman and chief executive officer's responsibilities, are provided by the

---

76 Companies Act 71 of 2008.
77 Werner Schoeman "Corporate Governance – Less is More" (2022) 36(2) *Speculum Juris* 414.
78 Werner Schoeman "Corporate Governance – Less is More" (2022) 36(2) *Speculum Juris* 414.
79 N Mans-Kemp, P Erasmus and S Viviers "Advances in the corporate governance practices of Johannesburg Stock Exchange companies" (2016) 20 *Southern African Business Review* 72.
80 Ibid footnote 79 at 75.
81 71 of 2008.
82 Monray Botha "The Role and Duties of Directors in the promotion of Corporate Governance: A South African perspective" (2009) *Obiter* 707.
83 2000 3 SA 806 (C).
84 Section 76(3) of the Companies Act 71 of 2008.
85 Ibid footnote 84.

Companies Act and the King Code.[86] Listed companies are required by the JSE Listings Requirements to maintain a balanced board structure, with a suitable proportion of both executive and non-executive directors.[87]

Sections 28, 29 and 30 of the Companies Act[88] addresses management control primarily through provisions related to financial reporting, accounting records, and internal control systems, section 28 deals with "Accounting Records", section 29 covers "financial statements" and section 30 addresses "annual financial statements".

Section 28(1)[89] states that

> "A company must keep accurate and complete accounting records in one of the official languages of the Republic— (a) as necessary to enable the company to satisfy its obligations in terms of this Act or any other law with respect to the preparation of financial statements; and (b) including any prescribed accounting records, which must be kept in the prescribed manner and form."

While section 28(2)[90] mandates that the accounting records must be kept at the company's registered office.

Section 29(1) of the Companies Act[91] requires "every company to produce annual financial statements within 6 months after the end of its financial year", section 29(2) specifies that "the financial statements must comply with applicable accounting standards and regulations", and section 29(3) outlines "the requirements for the financial statements to present fairly the company's state of affairs, financial results, and cash flows".

Additionally, section 30(1) of the Companies Act[92] "the financial statements to be audited by an independent auditor", and section 30(2) sets out "the responsibilities of the directors in relation to the financial statements, including taking responsibility for the preparation and fair presentation

---

86 Institute of Directors Southern Africa "General Guidance note: Board composition", available at *https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/49D62EF3-F749-403C-BE47-73C50F27F30F/General_Guidance_Note_on_Board_Composition.pdf*, accessed on 25 April 2025.

87 N Mans-Kemp, P Erasmus and S Viviers "Advances in the corporate governance practices of Johannesburg Stock Exchange companies" (2016) 20 *Southern African Business Review* 72.

88 71 of 2008.

89 Section 28(1) of the Companies Act 71 of 2008.

90 Section 28(2) of the Companies Act 71 of 2008.

91 Ibid footnote 88.

92 Ibid footnote 88.

of the statements". While section 30(3)(*c*) and 30(3)(*d*) of the Act[93] requires directors to accept accountability for the information contained in the company's financial accounts and to present them at the annual shareholders' meeting.[94]

The company's board of directors is largely responsible for upholding good governance norms, which serve as a foundation for corporate reporting and disclosure.[95] The audit committee's membership requirement that all members be non-executive directors of the business effectively places internal company auditor oversight under the purview and control of directors' governance.[96] The "apply-and-explain" method, which emphasises the values and goals of the governance code, is at the core of corporate governance disclosure.[97] According to the King Codes of Application and Disclosure,[98] non-compliance with the voluntary principles and leading practices implies that directors may be held legally liable and that a court may have to decide whether or not they fulfilled their governance obligations.[99]

Therefore, declaring Corporate Governance practices openly satisfies the need to see a company's governance and accountability mechanisms first-hand by giving outsiders, particularly investors, a window of opportunity to continuously monitor the quality of governance structures.[100] This demonstrates the managerial commitment to greater transparency, integrity, and financial disclosure.[101]

The following discussion now focuses on illustrations of effective and ineffective corporate governance practices in context of cyber security and data privacy.

---

93 Companies Act 71 of 2008.

94 Werner Schoeman "Corporate Governance – Less is More" (2022) 36(2) *Speculum Juris* 413.

95 See sections 29 and 30 of the Companies Act 71 of 2008 and Werner Schoeman "Corporate Governance – Less is More" (2022) 36(2) *Speculum Juris* 413.

96 Sections 94(4)(*a*) and 94(4)(*b*) of the Companies Act 71 of 2008.

97 Werner Schoeman "Corporate Governance – Less is More" (2022) 36(2) *Speculum Juris* 413.

98 Found in part 3 of the King IV Codes, see Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

99 Ibid footnote 99.

100 Collins Ntim, Kwaku Opong, Jo Danbolt "The Relative Value Relevance of Shareholder versus Stakeholder Corporate Governance Disclosure Policy Reforms in South Africa" (2012) 20(1) *Corporate Governance: An International Review* 88.

101 Ibid footnote 100.

2.2.1 IILUSTRATIONS OF EFFECTIVE CORPORATE GOVERNANCE PRACTICES

There are different illustrations that can be used to emphasise key facets of South Africa's, and other countries, successful corporate governance policies, highlighting the nation's dedication to moral, open, and inclusive business practices. A true involvement of directors and stakeholders that are involved in the management of the company, and well as the coordination of the many perspectives of stakeholders are prerequisites for effective corporate governance. In order to safeguard stakeholder rights and increase the company's value, effective corporate governance must be achieved for the stability, accountability and growth of a company.[102]

South Africa's corporate governance framework, primarily guided by the King IV Report on Corporate Governance,[103] emphasises several key prerequisites for effective governance. Here is how "education, technical proficiency, core competency, good communication, and Management Information System ("MIS")"[104] Contribute to corporate governance effectiveness in the South African context:

1. Education and technical proficiency: The Institute of Directors Southern Africa emphasises that board members must possess appropriate educational qualifications and technical expertise to fulfil their fiduciary duties effectively,[105] and section 76(3) of the Companies Act[106] requires directors to exercise their duties with the degree of skill and diligence reasonably expected from someone with their knowledge and experience.
2. Core competency: Directors should demonstrate competence in strategic planning and risk management,[107] and the JSE Listings requirements mandate that boards collectively possess appropriate industry knowledge and experience.[108]

---

102 Arti Aneja "Philosophy of Corporate Social Responsibility Vis-à-vis Corporate Governance" (2015) 6(7) *International Research Journal of Management Sociology & Humanity* 159.

103 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf,* accessed on 20 November 2023.

104 Arti Aneja "Philosophy of Corporate Social Responsibility Vis-à-vis Corporate Governance" (2015) 6(7) *International Research Journal of Management Sociology & Humanity* 158.

105 Ibid footnote 103.

106 71 of 2008.

107 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

108 Lexis Nexis "JSE Limited Listings Requirements", available at *https://www.jse.co.za/sites/default/files/media/documents/2019-04/JSE%20Listings%20Requirements.pdf*, accessed on 27 January 2025.

3. Good communication: Transparent and effective communication fosters trust among stakeholders, including employees, investors, and regulators.[109] In South Africa, where corporate scandals and governance failures have eroded public trust, clear communication is vital for rebuilding credibility and ensuring accountability.
4. MIS: MIS systems, such as the Risk Management Information System ("RMIS") provides the tools to collect, analyse, and report data essential for governance, including performance metrics, compliance tracking, and risk assessment.[110]

The Chief Executive Officer and Facilitator of the Institute of Directors ("IoDSA"), Parmi Natesan and Prieur du Plessis, stated that there is a strong foundation for corporate governance in South Africa.[111] The country's King Codes are highly acclaimed globally, and their different versions show the shift from a mindset of strict compliance to one that focuses on the use of moral leadership by the board of directors or other governing body to accomplish specific goals, such as a moral culture, high performance, efficient control, and legitimacy.[112]

The Sasol Limited ("Sasol") Sustainability Report 2021 offers information about the business's efficient corporate governance procedures, with a focus on data privacy and cybersecurity.[113] The report emphasises Sasol's implementation of the ISO 27001 Information Security Management System ("ISMS") standard throughout its activities and asserts that their ISMS offers a strong structure for handling cyber and information security risks, which showcases Sasol's dedication to proficient cybersecurity governance by following this globally acknowledged framework.[114]

Financial institutions, particularly banks, indicated in their reports that they have implemented effective corporate governance practices by establishing board-level oversight and risk management mechanisms specifically focused on cybersecurity. As part of its risk management

---

109 Nereida Hadziahmetovic, Nejla Salihovic "The Role of Transparent Communication and Leadership in Employee Engagement" (2022) 11(2) *International Journal of Academic Research in Economic & Management Sciences* 561.

110 Riskonnect "RMIS: The definitive guide", available at *https://riskonnect.com/resources/rmis-the-definitive-guide/*, accessed on 27 January 2025.

111 Parmi Natesan and Prieur du Plessis "Corporate Governance: South Africa's secret weapon", available at *https://www.iodsa.co.za/news/538251/Corporate-governance-South-Africas-secret-weapon.htm*, accessed on 24 February 2024.

112 Ibid footnote 111.

113 Sasol's sustainability report is available at *https://www.sasol.com/investor-centre/sustainability-reporting*, Accessed on 29 April 2024.

114 Page 54 of the Sasol Limited "June 2021 Sustainability report", available at *https://www.sasol.com/investor-centre/sustainability-reporting*, accessed on 29 April 2024.

mandate, Absa Group Limited ("Absa") has a Group Risk and Capital Management Committee that is responsible for overseeing the organisation's risk management procedures, which includes cybersecurity risks, this committee assesses and endorses the group's cybersecurity risk tolerance, risk management structures, and policies.[115]

However, a potential skills gap between the technical expertise of IT professionals and the risk governance knowledge of committee members can pose challenges in effective communication, risk assessment, strategy alignment, and talent management.[116] Bridging this gap through collaboration, cross-functional training, inclusion of cybersecurity experts, and aligning IT and risk management approaches is crucial for organisations to effectively manage their cybersecurity risks within the established risk tolerance levels.[117] According to the 2021 Integrated Report, the committee "evaluates the efficiency of the group's cybersecurity risk management procedures and verifies the implementation of suitable controls."[118]

Woolworths Holdings Limited ("Woolworths") stands out as a prime example of a South African company that upholds strong corporate governance principles and consistently aligns itself with the guidelines set forth in the King Codes, particularly in its board selection process. The company ensures a well-rounded and diverse board, comprising individuals with a blend of skills, experience, diversity, and independence to bolster effectiveness, as recommended by the King Codes.[119] It conducts regular assessments of the board's performance, its committees, and individual directors, facilitating the identification of areas for enhancement and ensuring ongoing effectiveness in its governance role and actively engages with its stakeholders to grasp their perspectives and integrate their feedback into its governance methodologies, a pivotal aspect emphasised by the King Codes.[120] Through its rigorous board selection and oversight procedures,

---

115 Absa Group Limited Integrated Report 2021, available at *https://www.absa.africa/wp-content/uploads/2022/09/Absa-Group-Integrated-Report.pdf*, accessed on 29 April 2024.

116 General principles of risk management and cybersecurity governance. See Anne Kohnke and Dan Schoemaker "Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control" (2015) 52:3 *Taylor & Francis* 10.

117 Anne Kohnke and Dan Schoemaker "Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control" (2015) 52:3 *Taylor & Francis* 10. ê

118 Absa Group Limited Integrated Report 2021, available at *https://www.absa.africa/wp-content/uploads/2022/09/Absa-Group-Integrated-Report.pdf*, accessed on 29 April 2024.

119 Woolworths Holdings Limited "Governance report 2022", available at *https://www.woolworthsholdings.co.za/wp-content/uploads/2022/09/Governance_Report_2022.pdf*, accessed on 29 April 2024.

120 Ibid footnote 119.

Woolworths demonstrates a steadfast commitment to robust corporate governance, setting a standard that other South African companies aspire to emulate.

Discovery Limited ("Discovery"),[121] is a South African company acknowledged for its proficient corporate governance approaches concerning cybersecurity and data privacy. Discovery has undertaken measures to guarantee full compliance with POPIA, encompassing the safeguarding of personal information handled by the company, and they have instituted protocols to fortify the security of both client and company data, shielding it from unauthorised access.[122] The company has developed an extensive cybersecurity framework that adheres to global standards, this framework comprises routine risk evaluations, the deployment of strong cybersecurity protocols, and continual surveillance and documentation of cybersecurity risks.[123] Discovery also offers clear and open reporting on its governance procedures, including cybersecurity, to stakeholders through its annual governance report.[124]

2.2.2 IILUSTRATIONS OF INEFFECTIVE CORPORATE GOVERNANCE PRACTICES

Ineffective corporate governance practices can expose companies to cyber threats, data breaches, and other security breaches, leading to significant repercussions. Several incidents within South African companies underscore the critical role of strong corporate governance frameworks in safeguarding against cybersecurity risks.

Cybersecurity in state-owned enterprises ("SOEs") is integral to socioeconomic development policy. Transnet serves as a prime example of an SOE whose vulnerability to inadequate cybersecurity measures could significantly harm the South African economy and further burden the disadvantaged and marginalised populations. In July 2021, Transnet experienced a significant cybersecurity breach that severely impacted its operations, resulting in widespread disruptions and financial losses, according to Transnet's own disclosure, the cyber incident involved a ransomware attack on its IT network.[125] Reports indicate that Transnet's board and executive

---

121 A financial services entity that operates across various sectors, including healthcare, life assurance, short-term insurance, savings and investment products, and wellness markets.

122 Discovery "POPIA: Protection of Personal Information Act", available at *https://www.discovery.co.za/corporate/popia-security,* accessed on 29 April 2024.

123 Discovery "POPIA: Protection of Personal Information Act", available at *https://www.discovery.co.za/corporate/popia-security,* accessed on 29 April 2024.

124 Discovery "Governance Report for the year ended 30 June 2023", available at *https://www.discovery.co.za/assets/discoverycoza/corporate/investor-relations/2023/discovery-governance-report.pdf,* accessed on 29 April 2024.

125 Scott Timcke, Mark Gaffley and Andrew Rens "The centrality of cybersecurity to socioeconomic

leadership neglected to prioritise cybersecurity measures and establish effective governance frameworks to effectively oversee and manage cyber risks.[126] This lack of oversight and accountability at the top level contributed to the company's vulnerability to the attack. Despite operating in a high-risk environment as a critical infrastructure provider, Transnet seems to have inadequately assessed and addressed its cybersecurity risks and overlooked the outdated systems and inadequate security measures made the company an appealing target for cybercriminals.[127]

A notable example is the data breach that took place at Liberty Holdings Limited ("Liberty") in 2018. This breach compromised the personal data of numerous customers, including their names, contact information, and identification numbers.[128] After investigations it was found that the breach occurred due to insufficient security protocols and a deficiency in effective governance frameworks for managing cybersecurity risks.[129] Another example is the incident involving Experian South Africa, a credit bureau, which encountered a data breach in 2020 and held at ransom.[130] This breach impacted millions of South Africans and exposed confidential personal and financial data, and subsequent investigations unveiled that the breach stemmed from an unsecured server, underscoring the necessity for enhanced governance measures concerning data security and access management.[131]

A study was conducted that examined the level of corporate governance violations that were made public and connected to agreements that were meant to support Broad-based Black Economic Empowerment ("BBBEE") at twenty-two different mining companies in South Africa.[132] These reported violations were evaluated using a framework created from pertinent laws and codes. The most often mentioned categories of behaviour encouraging violations in governance were interference in politics and nepotism, these were followed by fraud, structuring of contentious BEE transactions, and incompetence.[133]

---

development policy: A case study of cyber-vulnerability at South Africa's Transnet" (2023) *The African Journal of Information and Communication* 19.

126 Ibid footnote 125 at 20.

127 Ibid footnote 125 at 21.

128 Allison Job "Did one simple issue crash Liberty?", available at *https://www.itweb.co.za/article/did-one-simple-issue-crash-liberty/dgp45qaGabl7X9l8*, accessed on 29 April 2024.

129 Ibid footnote 128.

130 Joe Warminsky "South Africa credit bureau breached, data reportedly held for $15M ransom", available at *https://cyberscoop.com/south-africa-transunion-data-breach/*, accessed on 29 April 2024.

131 Ibid footnote 130.

132 Adele Thomas "Media-reported corporate governance transgressions in broad-based black economic empowerment deals in the South African mining sector" (2014) 8(2) *African Journal of Business Ethics* 89

133 Ibid footnote 132.

These incidents underscore various ineffective corporate governance practices related to cybersecurity in South African companies, such as lack of board-level oversight; insufficient risk assessment and management; inadequate policies and procedures; and lack of transparency and disclosure.

Moreover, the correlation between these high-profile debacles and the need for enhanced governance standards in South Africa underscores the relevance of initiatives like the King IV Codes[134] report and the Companies Act.[135] These regulatory frameworks provide guidelines and standards to promote transparency, accountability, and ethical conduct within South African companies, offering a roadmap for strengthening governance practices and fostering trust among stakeholders.[136] Through a comprehensive study of both negative and positive examples, South Africa can strive to cultivate a corporate culture rooted in integrity, responsibility, and sustainability.[137]

2.3 A SYNOPSIS OF THE LEGISLATION AND FRAMEWORK THAT GOVERN CYBERSECURITY

The downside of the Fourth Industrial Revolution's ("4IR")[138] lightning-fast digitalisation was a rise in a number of cyberattacks and crimes, which included "cyber fraud,[139] cyber extortion,[140] cyber forgery,[141] malicious property damage from computer viruses, child pornography, hacking,

---

134 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

135 71 of 2008.

136 Lindokuhle Ramalepe *Ethical Corporate Governance: The significance and impact of ethics in the South African Corporate Culture* (Unpublished Master's Degree in Governance and Political thesis, University of The Free State, 2021) 95.

137 Ibid footnote 136.

138 The fourth industrial revolution "describes a world where individuals move between digital domains and offline reality with the use of connected technology to enable and manage their lives." See Min Xu, Jeanne David and Suk Kim "The Fourth Industrial Revolution: Opportunities and Challenges" (2018) 9(2) *International Journal of Financial Research* 90.

139 Cyber fraud is the intentional misrepresentation that causes or risks harm, often seen in phishing and spoofing attacks. See Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 312.

140 Cyber extortion involves coercing someone to gain an advantage or force them to act or refrain from acting. Ransomware attacks are a common example, where criminals demand payment to restore access to encrypted data. See Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 314.

141 Cyber forgery is the intentional falsification of data or programs to harm or disadvantage another person. See Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 314.

cracking", among other online crimes.[142] Although some of these offenses may be handled by common law, it was obvious that illegal activity in cyberspace[143] needed to be governed by statute. As a result, the state legislature passed a new cybercrime law.[144]

Below is a discussion and analysis of these legislation and the role they play in governing cybersecurity in corporate.

2.3.1 ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 of 2002

The Electronic Communications and Transactions Act[145] ("ECTA") was promulgated in 2002 and an important source of inspiration for the cybercrime elements of this Act is the Budapest Convention on Cybercrime.[146]The Budapest Convention serves as a framework that enables numerous practitioners from participating countries to exchange knowledge and establish connections to enhance collaboration in particular instances, even extending to emergency scenarios, beyond the Convention's provisions.[147] Additionally, any country has the option to utilise the Budapest Convention as a reference, checklist, or template legislation.[148] It served as the principal piece of law that made cybercrimes illegal for almost twenty years.

The ECTA is integral to corporate governance in South Africa, as it provides a legal framework for electronic transactions, data protection, and cybersecurity. By legally recognising electronic signatures[149] and data messages,[150] the Act ensures that digital transactions are secure and enforceable, supporting efficient and compliant business operations. This fosters accountability and transparency, which are some of the key principles of good corporate governance.

Chapter 13 of the Act, sections 85 to 89, addresses cybercrime, outlining offenses such as unauthorised access to data, interception of communications, and cyber fraud. South African

---

142 Deepansh Kumar, Yugansh Khera, Nidhi Garg, *et al* "Towards the impact of hacking on cyber security" (2018) 9(2) *IIOAB Journal* 62.

143 Cyberspace is defined as "the collective mind and body of digital human society and intelligence." See Myles Garvey "A Philosophical Examination on the Definition of Cyberspace" (2021) *Cyber Security and Supply Chain Management* 8.

144 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 303.

145 Electronic Communications and Transactions Act 5 of 2002.

146 The Budapest Convention is available at *https://www.coe.int/en/web/cybercrime/the-budapest-convention*, accessed on 30 November 2023

147 Ibid footnote 146.

148 Ibid footnote 146.

149 Section 37 of the ECTA.

150 Section 11 of ECTA.

courts have applied these provisions in various cases to prosecute and convict individuals involved in cyber-related criminal activities as in *Okundu v S*[151] where the appellant was convicted on multiple counts, including contraventions of sections 86(1) and 86(4) of the ECTA. These sections pertain to unauthorised access to data and the use of devices to overcome security measures, respectively.[152] The court found that the appellant unlawfully accessed and manipulated data, leading to his conviction under these provisions.[153]

This Act has implemented particular cybercrimes laws. Chapter 13 of the Act, which deals with cybercrimes, makes the following actions illegal:

- Unauthorised access to information or interception of information;[154]
- Unauthorised intentional interference resulting in modification, rendering ineffective or destruction of information;[155]
- Overcoming security measures which protect data, including sale, distributions or possession of a device that is meant to overcome security measures;[156]
- A complete or partial denial of service attack;[157]
- Computer-related extortion, fraud or forgery;[158] and
- Attempt, and aiding and abetting in any of the abovementioned acts.[159]

Chapter IX of the Act regulates critical databases, which are deemed significant for safeguarding the Republic's national security or the economic and social welfare of its citizens. These databases must be registered and managed in accordance with ministerial directives, considering the security of the databases and the physical safety of those in charge of them. The Director-General audits this type of critical database management, and if non-compliance is discovered, the critical database administrator is notified of corrective action, if the administrator disregards the corrective action, they will be held accountable for a crime.[160]

---

151 *Okundu v S* (CA&R117/16) [2016] ZAECGHC 131 (22 November 2016).
152 Ibid footnote 151 at paragraph 6.
153 Ibid footnote 151.
154 ECTA S 86(1).
155 ECTA S 86(2).
156 ECTA S 86(3) and 86(4).
157 ECTA S 86(5).
158 ECTA S 87.
159 ECTA S 88.
160 Council of Europe "South Africa Cybercrime policies/strategies", available at *https://www.coe.int/en/web/octopus/-/southafrica#:~:text=The%20Government%20of%20South%20Africa,19%20of%202020*, accessed on 30 November 2023.

The Act has brought some successes with prosecuting certain cybercrimes. In the *R v Douvenga*[161] unreported case, which is among the first cases that examined the ECTA, for example, the defendant was found guilty of violating section 86(1) of the ECTA by knowingly and illegally gaining access to information that she knew was confidential and sent it to her fiancé via email. Another judgement that applied section 86 of the Act is in the *Salzmann v S*[162] case, where the court found that there is a serious crime under section 86(5) of the ECT Act. The prosecution contended that section 86(3) of the ECT Act created a new offense referred to as "anti-cracking (anti-thwarting) and hacking law", which also made it illegal for someone to own specific equipment and use them for purposes that are forbidden by section 86 (4) of the ECTA.

After South Africa not ratifying the Budapest Convention on cybercrime after signing it,[163] it became vital to prevent cybercrime and promote global collaboration and legislative framework harmonisation in Africa.[164] This was done through the African Union when it enacted the African Union Cyber Security and Protection of Personal Data Convention (also known as the "Malabo Convention") in 2014.[165] This Convention aims to synchronise the legal frameworks of African states for data protection, cybersecurity governance, cybercrime control, and electronic commerce.[166]

As one might expect, there has been a significant evolution of technology between the time the ECTA became law and today. The fields of AI, data mining,[167] blockchain technology,[168] internet

---

161 *R v Douvenga* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2002, unreported).

162 *Salzmann v S* (755/18) [2019] ZASCA 145; [2020] 1 All SA 361 (SCA); 2020 (2) SACR 200 (SCA) (13 November 2019).

163 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 304.

164 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 305.

165 The African Union enacted the African Union Cyber Security and Protection of Personal Data Convention Can be accessed on *African Union Convention on Cyber Security and Personal Data Protection | African Union (au.int)*, accessed on 4 February 2024.

166 Uchenna Jerome Orji "The African Union Convention: A regional response towards cyber stability?" (2018) 12(2) *Masaryk University Journal of Law and Technology* 98.

167 Data mining involves identifying irregularities, trends, and correlations within extensive datasets that enables the prediction of outcomes. It is to analyse and sift through large volumes of data to extract valuable insights. See Prasdika Prasdika and Bambang Sugiantoro "A review paper on Big Data and Data Mining concepts and techniques" (2018) 7(1) *International Journal on Informatics for Development* 33-34.

168 Blockchain technology, which is the foundation of Bitcoin, functions as an unchangeable record-keeping system that facilitates decentralized transactions. It also helps to diminish security vulnerabilities, eradicating fraudulent activities, and introducing an unprecedented level of transparency. See Zibin Zheng, Shaoan Xie and Hongning Dai *et al* "An overview of Blockchain Technology: Architecture, Consensus, and Future trends" (2017) *IEEE* 557 and Gousia Habib, Sparsh Sharma, and Sara Ibrahim *et al*

of things, and various other innovative technologies that were non-existent more than ten years ago are all heavily utilised in the 4IR. It became necessary for South African legislators to propose new legislation that kept up with these technical advancements,[169] which led to the promulgation of the Cybercrimes Act[170] to attend to some of these issues.

2.3.2 CYBERCRIMES ACT 19 of 2020

In 2021, the Cybercrimes Act was enacted as a law to address the contemporary issues facing the judiciary in light of the Malabo and Budapest Conventions. Sections 85, 86, 87, and 88 of the ECTA were repealed by chapter 2 of the Cybercrimes Act. Additionally, it substituted Section 89 of the ECTA, that dealt with penalties, in section 23 of the Cybercrimes Act with the previously indicated harsher sanctions. It is now one of the main laws establishing the offenses and punishments for cybercrime in South Africa.

The Act consists of 9 chapters and its Preamble states that "its purpose entails the creation of offences which have a bearing on cybercrime and to prescribe penalties for such crimes". It designates some offenses as cybercrimes, including: "unlawful access (section 2), unlawful interception of data (section 3), unlawful acts in respect of software or hardware tools (section 4), unlawful interference with data or computer programs (section 5), unlawful interference with computer data storage mediums or computer systems (section 6), unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data or device (section 7), cyber fraud (section 8), cyber forgery and uttering (section 9), cyber extortion (section 10) and theft of incorporeal property (section 12)".[171]

It introduces change to eleven critical pieces of legislation that govern cybersecurity, namely: The Criminal Procedure Act,[172] the South African Police Services Act,[173] the Films and Publications

---

"Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing" (2022) 14 *Future Internet* 1.

169 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 304.

170 19 of 2020.

171 These cybercrimes will be discussed in details in chapter three. See discussion in Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 307-312.

172 51 of 1977.

173 68 of 1995.

Act,[174] the Criminal Law Amendment Act,[175] the National Prosecuting Authority Act,[176] the Correctional Services Act,[177] the Financial Intelligence Centre Act,[178] the Electronic Communications and Transactions Act,[179] the Regulation of Interception of Communications and Provision of Communication Related Information Act,[180] the Criminal Law (Sexual Offences and Related Matters) Amendment Act,[181] and the Child Justice Act.[182]

Practically, companies must assess how their current systems relate to the Cybercrimes Act in terms of data management, especially in terms of database security and data encryption, manage identities and access, control wireless and network access, and handler passwords and privileges in accordance with the Act. How information is handled when employees depart an organisation is also one of the factors.[183]

South Africa has had numerous high-profile cyberattacks targeting some of the biggest companies in the nation these past few years, including vital national infrastructure.[184] These entities compromise the state-owned freight logistics company Transnet, which was the target of a ransomware extortion campaign by a hacking group based in Ukraine and Russia.[185] The Department of Justice and Constitutional development of South Africa also fell victim to a similar group in September 2021.[186]

More recently, in March 2022 extortionists with headquarters in in Brazil targeted TransUnion, one of the top credit bureaus in South Africa. A multitude of information was taken by the TransUnion attackers (including personal details such as identity numbers, employment information, gender, etc.) of customers who had registered with TransUnion. The hacking

---

174 65 of 1996.
175 105 of 1997.
176 32 of 1998.
177 111 of 1998.
178 38 of 2001.
179 25 of 2002.
180 70 0f 2002.
181 32 of 2007.
182 75 of 2008.
183 PR de Wet and David Olen "South Africa: The Cybercrimes Act, its relation with POPIA, and Compliance", available at *https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia*, accessed on 30 November 2023.
184 Makoma Toona "How the South African Cybercrimes Act 19 of 2020 will affect individuals and Businesses", available at *https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses*, accessed on 30 November 2023.
185 Ibid footnote 184.
186 Ridwaan Boda and Naledi Ramoabi "Data security breach: Information Regulator takes action against Department of Justice" available at *ENS - News - Data security breach: Information Regulator takes action against Department of Justice (ensafrica.com)*, accessed on 08 February 2024.

organisation (known as N4aughtysecTU) was reportedly demanding USD 14 million dollar (R224 million) in ransom.[187]

Section 3 of the Act addresses the offenses pertaining to personal information, such as the abuse of abuse, misuse, and possession of another person's or entity's personal information when there is a good faith to believe that it was used, or may be used, to perpetuate a cybercrime. It calls for the creation of multiple cybersecurity-related organisations, such as a national cybercrime center, a cyber response committee, and a 24/7 point of contact for all cybercrime reports.

Promoting cybersecurity awareness and education among the public and all stakeholders can contribute to better corporate governance and support directors in fulfilling their fiduciary duties. By fostering a more informed and security-conscious society, individuals are better equipped to recognise and mitigate risks associated with risky online behaviours, such as "phishing, cyberbullying, and weak password practices".[188] This can help reduce the overall cyber risk exposure for organisations, enabling directors to make more informed decisions and exercise due care in managing cybersecurity risks, which is a crucial aspect of their fiduciary responsibilities in today's digital landscape.

2.3.3 PROTECTION OF PERSONAL INFORMATION ACT 14 of 2013

Because of the increasing cases of theft and misuse of people's personal information, such as identity, medical and financial thefts, POPIA came into effect on 1 July 2020 to outline the Constitutional right to privacy.[189] The Act is a detailed privacy and personal data protection law in South Africa that places obligations on local and foreign organisations processing data in the nation regarding cybersecurity, and severely limits the export of personal data to other nations.[190]

Personal information is defined as "any information that may identify a person such as a name, surname, identity number, contact number, email address, religion, medical history, education,

---

187 Ridwaan Boda and Naledi Ramoabi "Data security breach: Information Regulator takes action against Department of Justice" available at *ENS - News - Data security breach: Information Regulator takes action against Department of Justice (ensafrica.com)*, accessed on 08 February 2024.

188 Elmarie Kritzinger, "Online safety in South Africa - A cause for growing concern" *2014 Information Security for South Africa*, Johannesburg, South Africa, 2014, available at *https://ieeexplore.ieee.org/document/6950502*, accessed on 30 November 2023.

189 Found in chapter 2, section 14 of the Constitution of South Africa, 1996.

190 ImmuniWeb "South Africa POPIA Compliance and Cybersecurity", available at *https://www.immuniweb.com/compliance/popia-compliance-privacy-cybersecurity/*, accessed on 29 November 2023.

financial, etc."[191] and data theft (information theft) is "the illegal transfer or storage of any information that is confidential, personal, or financial in nature, including passwords, software code, or algorithms, proprietary process-oriented information, or technologies."[192]

POPIA serves as one of the most important legislation for businesses because it protects data subjects from harm, or theft or discrimination. It requires companies to protect personal data in a suitable manner, penalties for violation of the Act can be harsh and include jail time and fines, hence neglecting to safeguard confidential information may result in a loss of clientele; money; and tarnished business image.[193] The Act created a lot of disruption to companies by imposing strict compliance requirements for data processing and other areas, companies were encouraged to use a customised approach to in the Act and avoiding box-ticking to guarantee meaningful compliance.[194]

The Constitution[195] protects the privacy of everyone and states in section 10 where everyone has the right to human dignity and for that dignity to the respected and protected. Section 14 also states that "everyone has the right to privacy, which includes the right not to have—

(a) their person or home searched;

(b) their property searched;

(c) their possessions seized; or

(d) the privacy of their communications infringed."

With the demand for competent workers in the defence and security sectors, in key national infrastructure, and in banking and finance, cybersecurity poses unique issues. All businesses will need to step up their cybersecurity efforts to the board level in order to comply with POPIA implementations.[196]

---

191 Section 1 of the Protection of Personal Information Act 14 of 2013.

192 Munish Sharma "Data Theft: Implications for Economic and National Security" (2017) 11(1) *Journal of Defence Studies* 62.

193 Tashreek Miller "Mitigate the Risk – Cybersecurity in South Africa", available at *https://fwblaw.co.za/mitigate-the-risk-cybersecurity-in-south-africa/*, accessed on 29 November 2023.

194 Ibid footnote 193.

195 The Constitution of the Republic of South Africa, 1996.

196 Ewan Sutherland "Governance of Cybersecurity – the case of South Africa" (2017) 20 *The African Journal of Information and Communication* 100.

Section 19 of POPIA requires responsible parties to implement "reasonable security measures" to protect personal data. However, the Act does not define what constitutes "reasonable" security or specify technical standards such as encryption levels, cybersecurity frameworks, or incident response protocols. This lack of clarity is a gap that forces businesses to interpret compliance requirements on their own, leading to inconsistent security practices and potential legal uncertainty.

Without explicit technical guidelines, enforcement by the Information Regulator may be inconsistent because organisations can argue over what qualifies as adequate protection. Unlike the European Union General Data Protection Regulation ("EU GDPR"),[197] which references standards like the ISO 27001,[198] POPIA leaves organisations without clear benchmarks for compliance. This gap increases the risk of weak data security measures and complicates compliance efforts for organisations navigating South Africa's evolving data privacy landscape.

Some of the strategic steps recommended for companies to take in order to comply with POPIA regulations are:

a) To ensure that all stakeholders understand the provisions of POPIA and its obligations regarding the use and processing of personal information and the rights of data subjects by training and educating them and keeping them updated with any POPIA changes or other relevant regulations to ensure ongoing compliance;[199]
b) Establish a clear and comprehensive Cybersecurity Policy by creating explicit directives for gathering, retaining, and discarding personal data that align with POPIA, this can include encompassing encryption, firewall protection, intrusion detection systems, and routine security upgrades;[200] and create and execute an incident response strategy to efficiently handle and minimise the impact of data breaches or security issues. This

197 The GDPR is a European Union law that protects the privacy of individuals' personal data. Available at *https://gdpr-info.eu/*, accessed on 29 January 2025.

198 ISO 27001 is the international standard for information security management developed by the International Organization for Standardization ("ISO"). Its adoption helps Companies in Europe to "establish, implement, operate, monitor, review, and manage an effective Information Security Management System ("ISMS")". See discussion in Isabel Maria Lopes, Teresa Guarda and Pedro Oliveira "Implementation of ISO 27001 Standards as GDPR Compliance Facilitator" (2019) 4(2) *Journal of Information Systems Engineering & Management* 3.

199 Kristyna Svobodova "POPI Act: The scope, purpose, and how to comply", available at *https://www.safetica.com/blog/popi-act-the-scope-purpose-and-how-to-comply*, accessed on 02 April 2024.

200 Oluwatoyin Akinbowale, Heinz Klingelhofer, Mulatu Zerihun, *et al* "Development of a policy and regulatory framework for mitigating cyber fraud in the South African banking industry" (2024) 10 *Heliyon* 3.

strategy must detail procedures for recognising, containing, and reporting security incidents in accordance with POPIA regulations.[201]

2.3.4 COMPANIES ACT 71 OF 2008 AND KING IV CODES ON CORPORATE GOVERNANCE

South African corporate law is mainly governed by the Companies Act[202] and King Codes on Corporate Governance.[203] The Companies Act was promulgated in April 2009, by replacing the former Companies Act 61 of 1973 and came into effect on 1 May 2011. The purpose of the Act is to "to provide for the incorporation, registration, management and capitalisation of profits in every company".[204]

Cyber dangers are growing on a nearly daily basis, offering several threats to businesses, and as a result, directors must stay up to date on laws and regulations in order to protect themselves and their organisations in their fiduciary roles. The duties of directors are outlined in section 77 of the Companies Act, Common law, and the King IV Codes on Corporate Governance in South Africa.[205]

The duty of a director in terms of section 76(3)(c) of the Act in conjunction with the King IV Codes, which is the benchmark for corporate governance in South Africa and is mandatory for any company that is listed on the JSE or aspires to be included on the JSE, requires a director to exercise a certain level of monitoring and comprehension over the cybersecurity and risks associated with the company's operations.[206]

The King IV Codes, published in November 2016, announced a dramatic shift in the way corporate governance is approached in light of the technological and digital advancements that

---

201 Pauline Meyer and Sylvain Métille "Computer security incident response teams: are they legally regulated? The Swiss example" (2022) 4 *International Cybersecurity Law Review* 39.

202 71 of 2008.

203 The King IV Report on Corporate Governance in South Africa is available on the Institute of Directors South Africa website, available at *https://www.iodsa.co.za/page/king-iv*, accessed on 20 November 2023.

204 As set out in the Preamble of the Companies Act 71 of 2008.

205 Section 77 of the Companies Act provides the statutory liabilities that are placed on directors of Companies and in terms of section 77(2) of the Act, a director "may be held liable (in accordance with the principles of the common law relating to the breach of a fiduciary duty) for any loss, damages or costs sustained by the company as a consequence of any breach by the director of the duties contemplated, inter alia, in section 76 of the Act".

206 Webber Wentzel "The liability of directors in cyberspace", available at *https://qa.webberwentzel.com/News/Pages/the-liability-of-directors-in-cyberspace.aspx*, accessed on 25 January 2024.

are reshaping company and changing goods, services, and companies. It exhorts organisations to fortify the procedures that support them, to prepare for change, and to react by seizing new possibilities and controlling emerging threats.[207]

Principle 12 of the King IV Codes focuses on information and technology governance and lays out seven specific guidelines which a business must follow. These include to:[208]

- Approve the policy for technology and information governance, including relevant frameworks and standards;
- Delegate the responsibility for effective implementation of technology and information management to management;
- Oversee the results of management's implementation, ensuring integration, business resilience, and risk monitoring related to cybersecurity, social media, third-party services, technology investments, and compliance;
- Supervise the management of information, focusing on use, architecture, privacy, and security;
- Oversee the management of technology, including architecture, sourcing risks, and disruptions;
- Consider independent assurance on the effectiveness of technology and information, including outsourcing; and
- Disclose a governance overview, including current and future focus areas, significant changes, acquisitions, and incident management monitoring.

The suggested practices place a strong emphasis on the necessity of accountability, ongoing supervision, and rules to guarantee information management and security.[209] Although the guidelines and suggested procedures do not specifically address a director's liability, they may raise expectations for their responsibilities, and more responsibilities may result in greater potential liability.

---

207 Institute of Directors Southern Africa "King IV report on corporate governance for South Africa 2016", available at *https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf*, accessed on 20 November 2023.

208 The King IV Report on Corporate Governance in South Africa is available on the Institute of Directors South Africa website, available at *https://www.iodsa.co.za/page/king-iv*, accessed on 20 November 2023.

209 Ibid footnote 208.

When a court considers whether a director acted with the adequate diligence, skill, and care required by the Companies Act, it is likely to take a look at the suggested practices and the director's compliance, or the absence thereof, if the director of a company disregards the 12 principles and the company experiences a cyber-attack that might have been preventable had the principles been followed. Therefore, King IV has interpretive power when deciding what a director is required to do by law, particularly when it comes to cybersecurity.[210]

2.4 DO THESE LEGISLATION PROVIDE ENOUGH SECURITY AND LEGAL PROTECTION FOR COMPANIES?

The goal of the cybersecurity legislation is to protect those who could be at risk of cybercrime and the functioning of decision-making processes in a way that promotes involvement, accountability, and transparency in the adoption of cyberspace-related measures, along with the framework of international agreements, strategies, laws, regulations, and standards that work best together, is known as cyber governance.[211]

South Africa needs to develop its own agenda for cyber governance, it needs a well-defined framework for cyber governance and a cohesive strategy could be beneficial.[212] Adhering to the Budapest Convention will primarily indicate the significance of cooperation in the field of cyber governance. This will be especially significant for global collaboration. African nations would have more options to obtain international support, as well as legal and technical aid, for improving cyber resilience in the area and advancing an agenda on cyber governance if they ratified the Budapest Convention. [213]

To safely conduct business and transactions, create institutions, and carry on with daily living in cyber environments, an essential aspect of modern society, a shared understanding and governing framework are required. Businesses and individuals can defend themselves against cybercrime by

---

210 Webber Wentzel "The liability of directors in cyberspace", available at *https://qa.webberwentzel.com/News/Pages/the-liability-of-directors-in-cyberspace.aspx*, accessed on 25 January 2024.

211 Serkan Savas and Suleyman Karatas "Cyber governance studies in ensuring cybersecurity: an overview of Cybersecurity governance" (2022) 3 *International Cybersecurity Law Review* 14.

212 Nnenna Ifeanyi-Ajufo "Cyber governance in Africa: at the crossroads of politics, sovereignty and Cooperation", available at *https://www.tandfonline.com/doi/full/10.1080/25741292.2023.2199960*, Accessed on 30 November 2023.

213 Nnenna Ifeanyi-Ajufo "Cyber governance in Africa: at the crossroads of politics, sovereignty and Cooperation" (2024) 6(2) *Policy design and practice* 154.

implementing adequate cybersecurity. Individuals, particular organisations, or a single nation cannot determine this framework. It is necessary to get the backing of the global regulatory and legally binding institutions. Naturally, there may be a technological shortcoming even though the policies that these institutions decide on their own tend to be sound.[214] As a result, the idea of democracy should consider the perspectives of all relevant parties, including academic institutions, the general public, the corporate sector, and individual users. Technology clusters ought to be included. Only with these kinds of solutions are long-term and forward-thinking actions possible.[215]

The ECTA establishes critical provisions for **c**ybersecurity, data protection, and the legality of electronic transactions. It addresses issues such as electronic signatures, data privacy, and cybercrime prevention. However, many of its provisions, particularly those related to cybersecurity and data privacy, were seen as outdated or insufficient, prompting the introduction of the Cybercrimes Act.[216] The Cybercrimes Act, which repealed certain chapters of the ECTA, aims to provide stronger measures to combat cybercrime, enhance corporate liability in cases of data breaches, and regulate offenses like unauthorised access to information. The Cybercrimes Act strengthens legal protection for companies by addressing emerging digital threats more comprehensively. While the Act provides foundational security and legal protection, it does not necessarily offer comprehensive security for companies in the face of evolving digital threats and complex cybercrimes such as cyber fraud and cyber extortion.[217]

There is a direct connection between the POPI Act and the Cybercrimes Act. The latter emphasises the privacy of data. Legal issues may arise from striking a balance between security, privacy, and individual freedom when quick investigations are required for cybercrimes. These can put to the test the extent of investigation authority as well as the data that judges and prosecutors are able to get.[218]

The Cybercrimes Act is a positive advancement in the criminal justice body of knowledge in South Africa. The Cybercrimes Act gives South African courts the authority to decide crimes in

---

214 Serkan Savas and Suleyman Karatas "Cyber governance studies in ensuring cybersecurity: an overview of Cybersecurity governance" (2022) 3 *International Cybersecurity Law Review* 31.

215 Ibid footnote 214.

216 19 of 2020.

217 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 313.

218 Karen Allen "South Africa lays down the law on cybercrime", available at *https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime*, accessed on 30 November 2023.

addition to designating specific behaviours as crimes. Authorities are also authorised to use their jurisdiction to conduct searches and obtain evidence. It should be mentioned that although though the legislation usually allows law enforcement officials to exercise their jurisdiction, they will still run across jurisdictional issues when trying to prosecute cybercrime.[219] These legislations may be able to provide companies with security against any cyberattacks and can protect all stakeholders, however, it is important for all companies to have frameworks that has procedures in place for when the company should experience any cyber-attacks and train all stakeholders on being cyber aware.

The Companies Act governs the corporate legal landscape in South Africa, focusing on corporate structure, duties, and responsibilities of directors, and providing mechanisms for transparency and accountability. While it addresses corporate governance and compliance, its scope is not deeply focused on cybersecurity or the protection of digital assets, which are critical for modern businesses. Companies are required to implement internal controls, but the Act does not explicitly mandate the use of cybersecurity measures or outline specific data protection protocols, this was also recognised as a gap in the new Companies Amendment Act[220] as it does not explicitly mandate comprehensive cybersecurity measures or the protection of digital assets, leaving companies to proactively implement additional measures to protect against cyber threats and ensure robust data security.

2.5 CONCLUSION

In conclusion, in light of South Africa's fast technological pace and growing reliance on digital platforms, the conversation on cybersecurity there highlights how crucial it is. Businesses have a great deal of issues due to the proliferation of cybercrimes, especially in light of the COVID-19 pandemic. Even though the government established the Information Regulator and passed laws like the Cybercrimes Act and POPIA to address cybersecurity concerns, there are still issues with service delivery that are caused by poor coordination, non-proactive risk assessments, and delays. The NCPF was adopted, but its poor implementation and lack of legislative scrutiny show that

---

219 Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 321.

220 16 of 2024.

more regulatory oversight and stakeholder cooperation are required to strengthen cybersecurity resilience.

CHAPTER THREE: CYBERCRIMES AND CYBERATTACKS IN CORPORATE GOVERNANCE

3.1 A PRECIS OF CYBERSECURITY

After having a look at the synopsis of the different legislation and frameworks that govern cybersecurity in South Africa, this chapter will identify and discuss those cybercrimes and cyberattacks that the legislation governs, the cyberethics thereof. It will also discuss how these cybercrimes and cyberattacks can be combatted, and how to develop an awareness culture for all stakeholders.

Although not specifically defined in the Cybercrimes Act, cybercrimes can take the form of unauthorised computer access, attacks on network privacy, and unauthorised interference with structures, programs, or information, it also covers fraud, theft, and forgery.[221] Cybersecurity includes cyber-risk management strategies, action plans, training, technology tools, and diplomatic measures to guarantee cyberspace safety use and involvement while containing cyber-threats.[222]

Africa is among the continents where cybercrime, exploitation, and other cybersecurity concerns are most prevalent. Because of the continent's abundance of cyber domains, growing end-user population, and the majority of African authorities' weak security frameworks, hackers see Africa as a safe sanctuary for their damaging cyber activities.[223] South Africa is the third highest hotspot for cybercrimes worldwide, rating after China and Russia.[224] According to reports, there were 230 million cyber threat discoveries in South Africa as of 2021, resulting in R2.2 billion in annual financial losses.[225]

---

221 Frederick Lemieux "Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives" (2011) *Developing Cyber Security Synergy* 1.

222 Oladotun E Awosusi "The imperative of Cyber Diplomacy and Cybersecurity in Africa: A new means to a Borderless Regional End?" (2022) 9(3) *Journal of African Foreign Affairs* 67.

223 Ibid footnote 222.

224 Ibid footnote 222 at 68.

225 Business Tech "South Africa under cyberattack: Interpol reveals top threats in South Africa", available at *https://businesstech.co.za/news/it-services/531990/south-africa-under-cyber-attack-interpol-reveals-top-threats-in-south-africa/*, accessed on 7 December 2023.

Poor cyber security interactions, poor cyber diplomatic efforts, and inadequate information networking infrastructure are the main causes of Africa's rising cyber threats and cybercrimes, the largest targets of cyberattacks, financial institutions, itself lack adequate cybersecurity procedures.[226]

An additional problem fuelling Africa's growing cyberthreats and cybercrimes is low cyberliteracy. Most online users and businesses lack the knowledge and abilities required to use the internet safely and avoid becoming targets for hackers.[227] There is a noticeable lack of cybersecurity knowledge on the continent. There appears to be a skills gap in cybersecurity across the region. There is an obvious scarcity of young cybersavvy individuals in Africa who could work as cyber workers to maintain cybersecurity across the continent.[228]

3.2 THE DIFFERENT CYBERCRIMES, CYBERATTACKS AND CYBERETHICS

The most frequent cyberthreats in Africa, according to the Interpol Assessment Report on Cybercrime,[229] is "Online scams, digital extortion, business email compromise, ransomware, and botnets".[230] These cyberthreats and concerns are also known as cyberethics, which relates to the moral guidelines for using technology and that understanding it is necessary to comprehend it.[231] A "one-size-fits-all" cybersecurity plan does not handle risks and cyberattacks, therefore companies should evaluate their security demands, requirements, and weaknesses.[232]

3.2.1 SOME OF THE DIFFERENT CYBERCRIMES AND CYBERATTACKS

It has been difficult to define cybercrime, with many meanings being applied in various situations because it is crucial to avoid restricting the definition to a certain category of technology because it would be very restrictive. A broad definition is necessary to accommodate emerging technology.

---

226 Oladotun E Awosusi "The imperative of Cyber Diplomacy and Cybersecurity in Africa: A new means to a Borderless Regional End?" (2022) 9(3) *Journal of African Foreign Affairs* 69.

227 Ibid footnote 226.

228 Ibid footnote 226.

229 Interpol "Interpol report identifies top cyberthreats in Africa" available at *https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa*, accessed on 7 December 2023.

230 Ibid footnote 229.

231 Joel Chigada and Rujeko Madzinga "Cyberattacks and threats during COVID-19: A systematic literature Review" (2021) 23(1) *South African Journal of Information Management* 10.

232 Ibid footnote 231.

Any illegal behaviour involving a computer, networked device, or network is referred to as a cybercrime. While the majority of cybercrimes are committed with the intention of making money for the perpetrators, some are committed specifically to harm or destroy computers or other devices. Cyberattacks are attempts to gain illegal entry to computer networks in order to steal, reveal, alter, remove, or damage the assets of others.

Some of the most common cybercrimes and cyberattacks that companies face on a daily basis and are found in chapter 2 of the Cybercrimes Act are:

a) Unlawful access ("hacking"): It involves gaining unauthorised access to computer systems of networks with the intent of stealing, modifying or damaging data for further attacks. Any purposeful, unauthorised access to computer systems or data devices that store data is prohibited. What it entails to access, use, and control computer programs and data is explained in section 2 of the Cybercrimes Act. The goal of the law is to stop illegal access to data and computer systems, which may result in further illegal activity.[233]
b) Phishing:[234] It is defined as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organisation in an automated fashion".[235] These behaviours frequently entail disclosing confidential information, such as credit card details or bank account numbers, downloading and installing dangerous software, and following links to phony websites. With the same fundamental goal, each type is distinguished by certain avenues and ways of implementation, such as phone, text, email, social media, etc.[236] Since the middle of the 1990s, hackers who utilise false emails to "fish for" information from unwary users have been referred to as "phishers". Phishing is a prevalent kind of cyberattack that targets people via phone calls, texts, emails, and other correspondence. The goal of a such an attack is to deceive the victim into doing the attacker's intended action, which could involve disclosing private data like username and password for a system or financial information.

---

233 Section 2 of the Cybercrimes Act of 19 of 2020.

234 Phishing is discussed widely by researchers, and because of its continuous evolution it does not have an established definition.

235 Jeffrey Proudfoot, Ryan Schuetzler, Justin Giboney, *et al* "Trends in Phishing Attacks: Suggestions for Future Research" (2011) 25 *Information Systems and Quantitative Analysis Faculty Proceedings & Presentations* 1.

236 Proofpoint "What is Phishing?", available at *https://www.proofpoint.com/us/threat-reference/phishing*, Accessed on 19 December 2023.

c) Unlawful interception of data: Whether the data is obtained directly or by the use of tools or techniques to intercept it, it is prohibited to capture or copy data from machines or their communication. Additionally, it is illegal to have such illegally obtained data in your hands or to have suspicious data in your possession without a valid reason. By limiting access to private data to permitted personnel exclusively, this section seeks to prevent unlawful access and interception of such information. Data interception is the act of obtaining, examining, recording, or replicating non-public data through the use of instruments such as hardware or software as mentioned in section 4(2) or through any other technique. In order to make the data accessible to someone other than the sender, recipient, intended recipient, or rightful owner, this is done. It also involves moving the data, or portions of it, off of its intended course and into another location, as well as looking at or reviewing the data's contents.[237]

d) Unlawful acts in respect of software or hardware tool ("Malware"): Malware, often known as malicious software, is defined as "a dangerous application harmful to personal internet-enabled devices and company systems"[238] and includes a wide range of destructive software, including Trojan horses, worms, viruses, and spyware.[239] Software and hardware instruments that are specifically created to facilitate actions that infringe the different provisions specified in the Cybercrimes Act are criminal to wilfully and illegally use or possess. These tools are designed to compromise computer systems, steal information, change information and programs, or obtain credentials and use them without authorisation. The purpose of section 4 of the Cybercrimes Act is to stop the unlawful utilisation of specialised technologies for online crimes and unauthorised activity.[240] This can be found in the case of *Ntozini v S*,[241] where a syndicate came up with a criminal plan to steal money from the Nelson Mandela Metropolitan Municipality ("NMMM") by installing programs for computers on NMMM's Corporate Access Terminal System and secretly captured data and send them to an email address belonging to a syndicate member.[242]

---

237 Section 3 of the Cybercrimes Act 19 of 2020.

238 Joel Chigada and Rujeko Madzinga "Cyberattacks and threats during COVID-19: A systematic literature Review" (2021) 23(1) *South African Journal of Information Management* 6.

239 TechTarget "Malware", available at *https://www.techtarget.com/searchsecurity/definition/malware#:~:text=Malware%2C%20or%20malicios*, Accessed on 19 December 2023.

240 Section 4 of the Cybercrimes Act 19 of 2020.

241 *Ntozini v S* (CA&R 05/2020) [2020] ZAECGHC 104 (15 September 2020).

242 Annalise Kempen "Are we making progress in the fight against cybercrime?" (2016) *Servamus* at 19.

e) Unlawful interference with data or computer program: Making deliberate and illicit changes to computer programs or data is prohibited. It encompasses operations like as erasing, altering, destroying, making inoperable, interfering with the operation of, or preventing access to data or software that is kept on computers or storage devices. The purpose of this section is to stop unauthorised access to electronic data, which might lead to system failures, data loss, or interruptions to digital services.[243]

f) Unlawful interference with computer data storage medium or computer systems: Intentional and illegally interfering with computer systems or storage is prohibited. This covers activities that could impair their functionality, harm them, interfere with their ability to protect confidential information, jeopardise the veracity of the information, or stop them from being useful. Preventing unauthorised actions that may result in issues with computer systems as well as information storage is the aim of this legislation.[244]

g) Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device: Passwords, access codes, and similar tools may not be obtained, unlawfully obtained, distributed, or used with the aim to violate the regulations specified in the aforementioned sections. Additionally, it becomes illegal if someone is discovered in possession of such tools and there is a plausible suspicion that they were meant for illegal purposes and they are unable to provide a convincing justification for their possession. The goal of the law is to stop these kinds of tools from being used for cybercrimes and unauthorised access to systems and data.[245]

h) Cyber fraud ("Ransomware"): Demanding money to prevent a threatened attack or release of data. Purposefully and fraudulently misleading someone by utilising computer-related techniques. This could entail utilising fraudulent information, altering data, or tampering with computer systems or software in order to defraud people out of their money.[246]

i) Spoofing: Where cybercriminals pose as reputable or well-known sources. Spoofing can take many different forms, including fake calls, spoof emails, Internet Protocol ("IP") spoofing, Address Resolution Protocol ("ARP") spoofing, GPS spoofing, and website spoofing.[247]

---

243 Section 5 of the Cybercrimes Act 19 of 2020.

244 Section 6 of the Cybercrimes Act 19 of 2020.

245 Section 7 of the Cybercrimes Act 19 of 2020.

246 Section 8 of the Cybercrimes Act 19 of 2020.

247 Bart Lenaerts-Bergmans "What is spoofing attacks?", available at *https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/*, accessed on 19 December 2023.

j) Online fraud or scams: A variety of dishonest online operations, including fraud involving advance fees, phony auctions, online shopping, and investment schemes that target victims' private data or money.[248]

k) Insider threats: These threats arise when people who have been granted authorised access to systems or data abuse that access for their own personal gain or to cause harm to their business, this is usually done by stealing confidential data or causing harm. These actions can be harmful and greatly raise the likelihood of major harm being done to the company's infrastructure or data systems privacy, reliability, or accessibility.[249]

A section 19 POPIA breach can be seen in an incident that accrued on May 2023, where the Information Regulator ("Regulator") publicly announced that it issued an administrative fine to the Department of Justice ("Department") of R5 million for contravention of sections 19 and 20 of POPIA.[250] This started when the Department struggled with their IT systems on September 2021 which resulted in their work systems being unavailable and the employees not bring able to work on the systems and assist the public, and lost roughly 1204 files that had personal information due to a hack.[251] The issue was due to the Department failing to implement sufficient technical safeguards to identify and track illegal access to data under its control. The Regulator also discovered that the department failed to update a number of licenses, which had expired in 2020, for technologies that could have assisted the Department in preventing the data breach. In addition, the Department neglected to set up and keep up proper defences against the dangers that ought to have been recognised. As a result, the Department was unable to continually update and monitor its security measures against malware attacks.[252]

---

248 Fortinet "Internet fraud", available at *https://www.fortinet.com/resources/cyberglossary/internet-fraud#:~:text=The%20term%20%22internet%20fraud%22%20generally,scam%20people%20out%20of%20money*, accessed on 19 December 20203.

249 Carol Silaule, Lean Makhubele, Stevens Mamorobela "A model to reduce insider cybersecurity threats in a South African telecommunications company" (2022) *South African Journal of Information Management* 1.

250 Legal practitioners, Ridwaan Boda and Naledi Ramoabi, at ENS Africa, an African law firm, published an article with the assessment of the fine issued by the Information Regulator and is available at *ENS - News - Data security breach: Information Regulator takes action against Department of Justice (ensafrica.com)*, accessed on 08 February 2024.

251 Ibid footnote 250.

252 Ridwaan Boda and Naledi Ramoabi "Data security breach: Information Regulator takes action against Department of Justice" available at *ENS - News - Data security breach: Information Regulator takes action against Department of Justice (ensafrica.com)*, accessed on 08 February 2024.

The Department used this as an opportunity to caution all public and private institution of the consequences for not notifying them of any data breaches that are contravention of POPIA and the Cybercrimes Act.

3.2.2 LEGAL ETHICS IN CYBERSECURITY: AN OVERVIEW

As mentioned in previous chapters above, ethics, which originates from the Greek word "*ethos*," refers to "a system of moral principle that compels a person to follow a specific action". It is a direction for behaviour concerning moral problems,[253] and is defined by as "the analysis of human actions from the perspective of good and evil, or of morally correct and morally wrong."[254]

For businesses to exist in many different nations and areas, business ethics are crucial.[255] Companies that want to be viewed as ethical use a variety of tools, such as codes of ethics, ethical standards, and ethical principles. But in reality, these businesses frequently conduct business entirely differently.

Cyberethics is a field of study that combines the above worries about cyberthreats with an emphasis on the impact of technology on ethical, legal and social systems.[256] It looks at laws and policies have been developed in response to issues arising from the growth and application of cybertechnology.[257] In cyber ethics, researchers classify hackers[258] according to their goals and methods. The three categories for hackers that are based on the motives behind their conduct are white hat hackers, black hat hackers, and grey hat hackers.[259]

---

253 WG Evans "Ethics, values and practice" (2019) 74(6) *South African Dental Journal* 333.

254 Christoph Bartneck and Christoph Lutge "What is ethics" in Christoph Bartneck, *et al* (eds) *An Introduction to Ethics in Robotics and AI* (2021) 17-26.

255 Włodzimierz Sroka and Marketa Lőrinczy "The perception of ethics in business: analysis of research Results" (2015) 34 Procedia Economics and Finance 156.

256 Aderinola Dunmade, Adeyinka Tella and Uloma Onuoha "Cyberethics awareness and implications on Library and Information Science educators in selected Universities in South-West Nigeria" (2023) 89(1) *South African Journal of Libraries and Information Science* 3.

257 Ibid footnote 256.

258 A hacker is often seen as "a slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s)". See Pieter Bezuidenhout "An IT auditor's view of a hacker's methodology" (2005) 2005(22) *Auditing SA* 25.

259 Denitsa Kozhuharova, Atanas Kirov and Zhanin Al-Shargabi "Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?" (2022) *Cybersecurity of Digital Service Chains* 205-207.

White hat hackers are ethical hackers,[260] who often get hired by various businesses to test their security systems and identify security flaws. For instance, in order to identify any potential vulnerabilities for a weakness in security, a team of white hat hackers would use techniques that are identical to those used by criminal hackers. But this is done to identify any weaknesses and develop procedures for solving them, and not to harm or steal data.[261]

Black hat hackers are hackers who engage in illicit system hacking. Their goals while breaking into a system without authorisation are to compromise its functionality or steal confidential or sensitive business data. In addition, they have the ability to compromise privacy, obstruct system network connectivity, and overburden the system to the point of slowness.[262]

Grey hat hackers operate at the middle ground of white and black hat hackers, making their actions spark the most ethical discussions. They take advantage of a security flaw in a computer system or network for their own amusement, acting without malice. Their goal in working is to make the owners aware of their weaknesses so they can offer their gratitude or a modest reward.[263] For example, to alert the owner to a security flaw in their network, this hacker may use the internet to browse and breach a computer system.[264]

3.3 HOW CYBERCRIMES AND CYBERATTACKS ARE COMBATTED

Cyberlaw seeks to lower risk and safeguard network security, while cybersecurity needs to be mitigated or minimised as a risk for the company. The basic norm is that "it is not if, but you will be hacked", and this requires for businesses to quickly recover from any attacks and have a business continuity strategy with cloud computing as a recommended option. Many companies, like financial institutions, have made cybersecurity and data privacy a top priority in order to

---

260 Ethical hacking usually focuses on safeguarding and preserving the company's computer systems, related equipment, and private data. See Shivanshi Sinha and Yojna Arora "Ethical hacking: The story of a white hat hacker" (2020) 8(3) *International Journal of Innovative Research in Computer Science & Technology* 132.

261 Denitsa Kozhuharova, Atanas Kirov and Zhanin Al-Shargabi "Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?" (2022) *Cybersecurity of Digital Service Chains* 206.

262 Mikhail Shlyakhtunov "White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies" (2021) 12(8) *International Journal of Advanced Computer Science and Applications* 430.

263 Ibid footnote 262.

264 Ibid footnote 262.

comply with legal obligations, increase in security breaches, and to meet their consumer commitments.[265]

In order to mitigate these risks, cybersecurity professionals need to have improved scenario design simulation, and the use of Breach and Attack Simulations ("BAS") to assess cyber resilience is becoming more widespread as technology works in a manner similar to continuous, automated hacking in that it can identify vulnerabilities in an organisation's cyber security.[266]

Because cybercriminals do not leave a standard crime scene in the same sense that a murder, for instance, leaves behind a body, bullet casings, or collectible Deoxyribonucleic acid ("DNA") evidence, investigators that investigate cybercrime must instead concentrate on computers, networks, and telephones. They might additionally be dealing with a victim in a particular country and a suspect in a different one, which makes it difficult to make connections and find an anonymous offender abroad. This implies that law enforcement must be aware of such possible circumstances.[267] Building a cybercrime ability at police stations might be a useful step, as this would allow police officers to do basic tasks, such as being taught in the proper way to seize possible evidence and report a case for particular investigation.[268]

According to the NCPF, the South African Police Services will be in charge of preventing, looking into, and fighting cybercrime.[269] This includes creating policies and strategies, interacting with stakeholders, offering specialised investigative capacity, creating and maintaining enforcement capabilities, and enhancing the South African Police Services fundamental knowledge of cybercrime.[270]

---

265 Yonnique Hanusch "Financial institutions should decline hackers' requests for voluntary compensation" (2021) 40(2) *South African Journal of Philosophy* 162.

266 Redscan "Breach and Attack Simulation", available at *https://www.redscan.com/services/breach-and-attacksimulation/#:~:text=A%20breach%20and%20attack%20simulation%20is%20a%20type%20of%20advanced,be%20used%20by%20malicious%20actors*, accessed on 12 December 2023.

267 Annalise Kempen "Are we making progress in the fight against cybercrime?" (2016) *Servamus* 19.

268 Ibid footnote 266 at 20.

269 Ibid footnote 266 at 2.

270 Ibid footnote 266 at 2.

3.4 FOSTERING A CULTURE OF CYBERSECURITY AWARENESS AND TRAINING WITH DIFFERENT STAKEHOLDERS

Businesses face an increasing danger of cyberattacks in the digital age, which forces them to take extra precautions to protect their assets, and creating an awareness and providing training on the matters of cybersecurity is one of the primary focus for businesses and government.

Although corporate culture plays an extensively studied and widely evidenced part in cybersecurity, its importance has increased recently as a result of the increasingly dangerous landscape. Businesses today accept and understand that using technology alone is not enough to protect against cyberattacks, which led them to implement more aggressive and modern procedures to successfully stop and lessen cyberthreats.[271]

3.4.1 HOW A CULTURE OF CYBERSECURITY AWARENESS CAN BE FORSTERED

One approach to resolving cyberattacks is to help communities and companies cultivate a strong cybersecurity culture. Cybersecurity culture encompasses the principles, dispositions, and actions that encourage security consciousness and optimal procedures among staff members, partners, and consumers.[272] In order to reduce the dangers of cybercrime, a strong cybersecurity culture may promote accountability, boost resilience, and create an atmosphere of shared accountability for cybersecurity.[273]

However, companies prioritise increasing technology investments to defend against external cyberattacks, often overlooking the importance of addressing insider threats.[274] Neglecting the roles and behaviours of users undermines the effectiveness of cybersecurity measures, as internal threats from employees and other stakeholders can significantly disrupt the organization's computer systems.[275]

---

271 Michael Mncedisi Willie "The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture" available at *https://www.researchgate.net/publication/371399113_The_Role_of_Organizational_Culture_in_Cybersecurity_Building_a_Security-First_Culture*, accessed on 04 February 2024.

272 Banuka De Silva "Exploring the Relationship between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review" (2023) 12(1) *International Journal of Information Security and Cybercrime* 24.

273 Ibid footnote 272.

274 Carol Silaule, Lean Makhubele and Stevens Mamorobela "A model to reduce insider cybersecurity threats in a South African telecommunications company" (2022) *South African Journal of Information Management* 1.

275 Anil Lamba, Satinderjeet Singh, Balvinder Singh *et al* "Analyzing and fixing Cyber Security Threats for

Moreover, insufficient attention is given to mitigating cybersecurity risks posed by insiders, hindering efforts to enhance security posture and cultivate a culture of security awareness within the organisation.[276] While organisations acknowledge the potential impact of insider threats on business operations, there is a need for a comprehensive, interdisciplinary approach that considers both the technological and human aspects of cybersecurity insider threats.[277] Detecting, preventing, or minimising these threats proves challenging for organisations, necessitating a holistic perspective to effectively manage cybersecurity risks when fostering a culture of cybersecurity awareness.[278]

A company can develop a strong cybersecurity culture by implementing procedures such as:

1. Developing a comprehensive cybersecurity policy framework: This framework establishes the different protocols, norms, and directives that must be adhered to. It provides a base on which staff members of an organisation can construct a shared comprehension of the risks, obligations, and guidelines related to cybersecurity. A thorough policy structure covering all facets of cybersecurity should include "access control, data protection, incident response, and employee training". [279]
2. Developing a culture that is supportive of cybersecurity: When employees understand the importance of cybersecurity and take ownership of their role in maintaining the integrity of the system, the culture is more likely to promote good attitudes toward the subject. It comprises encouraging a culture of openness and trust, rewarding good cybersecurity behaviour, and elevating users' feeling of shared accountability.[280]
3. Providing programmes for both training and awareness in cybersecurity: The primary line of safety against any prospective cyberattacks is a company's workforce. Consequently, it is imperative to provide them with the requisite information, abilities, and consciousness to identify and avert cyber hazards. Training and awareness initiatives should address the most recent risks in addition to suggested protocols and secure behaviour standards.[281]

Supply Chain Management" (2017) 4(5) *International Journal for Technological Research in Engineering* 5681.

276 Ibid footnote 275.

277 Ibid footnote 275.

278 Carol Silaule, Lean Makhubele and Stevens Mamorobela "A model to reduce insider cybersecurity threats in a South African telecommunications company" (2022) *South African Journal of Information Management* 1.

279 Annalise Kempen "Are we making progress in the fight against cybercrime?" (2016) *Servamus* 25.

280 Ibid footnote 279 at 24.

281 Banuka De Silva "Exploring the Relationship between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review" (2023) 12(1) *International Journal of Information Security and*

4. Implementing a cybersecurity strategy that is based on risk: When it comes to cybersecurity, a risk-based strategy prioritises and distributes resources and efforts according to the risk that each particular threat poses. It comprises developing risk management plans, implementing risk mitigation techniques, and doing risk assessments on a regular basis. With the help of this tactic, organisations may focus their energies and resources more effectively on the biggest cybersecurity threats.[282]

It can be challenging to create a culture that values cybersecurity since it involves a wide range of stakeholders, including users, suppliers, staff members, and leadership,[283] however, it is important for all stakeholders to find ways to develop a healthy cybersecurity culture that can be a shield to all attacks that are faced on a daily basis in the company. According to research, businesses a strong cybersecurity culture are more likely to recognise and respond rapidly to cyberattacks and there was less chance of an attack on these types of businesses.[284]

3.5 CONCLUSION

In conclusion, this *précis* offered a brief overview of the complex field of cybersecurity, covering a range of cybercrimes, cyberattacks, and cyberethics issues. Strong cybersecurity procedures are essential to secure digital assets and guard against risks to finances, reputation, and privacy since cyber threats, such as ransomware; phishing; malware; and social engineering, are always changing.

This chapter also highlighted the significance of developing an efficient cybersecurity culture in order to lessen the risks related to cybercrime. Strong cybersecurity cultures can improve resistance to cyberattacks, encourage accountability among people and organisations, and create a sense of shared responsibility for cybersecurity, among other advantages. Through the implementation of a culture that places a high priority on cybersecurity measures and promotes

---

Cybercrime 24.

282 Banuka De Silva "Exploring the Relationship between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review" (2023) 12(1) *International Journal of Information Security and Cybercrime* 26.

283 Banuka De Silva "Exploring the Relationship between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review" (2023) 12(1) *International Journal of Information Security and Cybercrime* 26.

284 Ibid footnote 283.

proactive risk management, stakeholders can collaborate to successfully tackle the obstacles presented by cybercrime and establish a digital environment that is safer.

CHAPTER FOUR: LEGAL AND ETHICAL IMPLICATIONS OF CYBERSECURITY AND PRIVACY LAWS

4.1 INTRODUCTION

This chapter will analyse the legal and ethical implications of cybersecurity and privacy laws within the evolving and often contentious political landscape of cyberspace, shaped by conflicting interests, norms, and values.[285] Additionally, it will explore how African cyberspace lacks a defined stable structure and largely unregulated domain, presenting both significant opportunities and risks. It is a sphere of non-physical global borders that links states and non-states entities as well as citizens, creating a variety of interactions and conflicts within and among them.[286] In actuality, cyberspace is a developing frontier full of opportunities and dangers. Due to its borderless character, it has become an "open domain" where non-state players have significant power which has led to organised crimes, threats, and attacks with enormous financial and human cost implications for people all over the world.[287]

Companies are always at great risk of cyberattacks. A cyberattack on a company that exposes private or sensitive information could have a number of negative effects on it, such as financial loss resulting from money that has been stolen; client complaints from the company's violation of the privacy policy; lawsuits for breach of contract where the company fails to fulfil contractual duties by abiding by data privacy laws; regulatory penalties for failure to comply with data privacy laws; and reputational damage from clients losing trust in the company's capacity to securely handle their personal information.

As cybersecurity threats, global issues, and consequences change, so do the ways in which cyberspace is explored and engaged. For example, approximately, 9 million South Africans fell victim to cyberattacks between January 2016 and September 2017, with approximately 23 percent of them over 55 years of age saying they experienced cyberattacks within that time.[288] Additionally, it appears that financial institutions in South Africa and certain government agencies

---

285 Andre Barrinha and Thomas Renard "Cyber-diplomacy: the making of an international society in the Digital age" (2017) 3 *Global affairs* 353.

286 Oladotun E Awosusi "The imperative of Cyber Diplomacy and Cybersecurity in Africa: A new means to a Borderless Regional End?" (2022) 9(3) *Journal of African Foreign Affairs* 71.

287 Ibid footnote 286 at 58.

288 Chiji Ezeji, Adewale Olutola, and Paul Bello "Cyber-related crime in South Africa: Extent and perspectives of state's roleplayers" (2018) 31(3) *Acta Criminologica: Southern African Journal of Criminology* 99.

are vulnerable to cyber threats due to insufficient oversight and the misuse of system rights.[289] These approaches also consider the misuse of privileged access by independent contractors, third parties, and outsourced service providers.[290]

According to a report, African countries that have a huge rate of population using cyberspace are: 86% in South Africa, 60% in Kenya, and 56% in Nigeria, respectively.[291] Opportunities-wise, cyberspace has had a significant impact on the continent in a number of ways. It has been extremely beneficial for the continent in regards to e-commerce, e-governance, e-education, and social media connections amongst and among Africans in addition to fostering intra-African trade.[292] It has also opened Africa up in terms of sharing data and technical skill development, giving African adolescents "open" job prospects and a chance to contribute to the continent's economic progress.[293]

4.2 LEGAL IMPLICATIONS OF CYBERSECURITY AND PRIVACY LAWS

Privacy is one of the main legal implications of Privacy law is the protection of personal and private information. A fundamental right that is necessary for maintaining human dignity is privacy. Large data volumes are frequently provided to AI systems so they may analyse and learn from them. The right to privacy is impeded by the collecting of data.[294]

At present, African nations lack a cohesive regulatory framework governing AI at both national and regional levels, and without appropriate legislation and policies in place to foster competition, data interoperability, and safeguards within data ecosystems, the risks associated with AI adoption could overshadow its potential benefits.[295] The introduction of AI brings forth certain challenges

---

289 This was discussed in an assessment of the current cyber threat faced by financial institutions in conducted by the World Bank, available at *https://documents1.worldbank.org/curated/en/099830405172214598/pdf/P1647700060153076 0af01093740e385fe8.pdf*, accessed on 07 April 2024.

290 Ibid footnote 289.

291 See John Campbell "Last Month, Over Half-a-Billion Africans Accessed the Internet", available at *https://www.cfr.org/blog/last-month-over-half-billion-africans-accessed-internet*, accessed on 12 May 2024 and Oladotun E Awosusi "The imperative of Cyber Diplomacy and Cybersecurity in Africa: A new means to a Borderless Regional End?" (2022) 9(3) *Journal of African Foreign Affairs* 66.

292 Oladotun E Awosusi "The imperative of Cyber Diplomacy and Cybersecurity in Africa: A new means to a Borderless Regional End?" (2022) 9(3) *Journal of African Foreign Affairs* 66.

293 Ibid footnote 292.

294 Willem Gravett "The dark side of Artificial intelligence: Challenges for the Legal System" (2020) 35(1) *University of South Africa Press* 5.

295 Caroline Ncube, Desmond Oriakhogba, Tobias Schonwetter *et al* "Artificial Intelligence and the law in

and risks, such as rendering traditional economic models driven by exports obsolete, exacerbating the existing digital and technological disparities, and fuelling concerns around data security, privacy infringement, and eroding public confidence in AI technologies.[296]

The first issue to bring up in discussions about AI is how hard it is to define AI legally and place it inside the framework of human rights. The utilisation of AI technologies can play a pivotal role in furthering fundamental human rights across Africa, such as the rights to healthcare, education, and children's welfare. Despite some cases where AI implementation has perpetuated technological biases and infringed upon data privacy, AI can also be leveraged as a tool to uphold and safeguard certain human rights principles.[297] When deployed responsibly and ethically, AI applications hold the potential to drive progress in realizing and protecting essential rights for individuals throughout the African continent.[298] AI can also create a legal implication of an AI surveillance state, where human behaviour is increasingly controlled and observed by machines, known as a "society of control". This is one conceivable result of these new technology advancements under more stringent state supervision.[299]

A significant legal consequence arising from the advancement of AI is the proliferation of disinformation. AI technologies can enable the creation of "deep fakes", which are highly realistic artificial images and videos, these deep fakes leverage automated learning techniques to synthesize voices and faces, seamlessly integrating them into genuine audio and video recordings of individuals.[300] By piecing together these digital fragments, AI facilitates the generation of strikingly lifelike impersonations, amplifying the potential for disseminating deceptive and misleading content on a large scale.[301]

In order to create regulatory frameworks for addressing the difficulties and seizing the potential that AI presents for the African continent, national and regional government forums have launched a number of legislative and policy efforts.[302] For instance, the Centre for AI Research ("CAIR")[303] in South Africa was founded in 2011 with financial support from the country's

---

Africa" (2023) *LexisNexis* 2-8.

296 Caroline Ncube, Desmond Oriakhogba, Tobias Schonwetter *et al* "Artificial Intelligence and the law in Africa" (2023) *LexisNexis* 8.

297 Ibid footnote 296

298 Ibid footnote 296.

299 Ibid footnote 296 at 10.

300 Ibid footnote 296 at 7-8.

301 Ibid footnote 296 at 7-8.

302 Ibid footnote 296 at 2.

303 CAIR is a "distributed South African research network with nine established and two emerging research

government, and is overseen by the Center for Scientific and Industrial Research ("CSIR")[304] in South Africa which consists of universities and other research organisations.[305]

Starting from 2022, preparations have been made to create a dedicated AI policy in Nigeria,[306] previously, in 2020, the National Centre for AI and Robotics ("NCAIR") was founded by the Nigerian National Information Technology Development Agency ("NITDA")[307] to "promote research and development on emerging technologies" and to guarantee that the technologies are used in a way that complies with the National Digital Economy Policy and Strategy 2020–2023 ("NDEPS").[308]

Similar to this, the World Economic Forum ("WEF") and Rwanda collaborated to establish the Center for the Fourth Industrial Revolution ("C4IR Rwanda") in 2020. Working with partners, C4IR Rwanda is entrusted with creating new legal frameworks for the regulation of new technologies and the commercial models they enable, in accordance with Rwanda's national development aspirations.[309]

4.3 ETHICAL IMPLICATIONS OF CYBERSECURITY AND PRIVACY LAWS

As mentioned previously, "ethics" refers to "a system of moral principle that compels a person to follow a specific action" and a direction for behaviour concerning moral problems.[310] These rules are frequently influenced by responsibilities, rights, and rewards.[311] Our understanding of the world around us is shaped by a few basic ethical concepts.

---

groups across eight universities funded primarily by the Department of Science and Innovation ("DSI")", available at https://www.cair.org.za/about, accessed on 04 April 2024.

304 CSIR is "a leading scientific and technology research organisation that researches and develops transformative technologies to accelerate socioeconomic prosperity in South Africa." Available at *https://www.csir.co.za/*, accessed on 07 April 2024.

305 Supra footnote 274 at 4.

306 OECD, available at *https://www.oecd.org/countries/nigeria/*, accessed on 26 February 2024.

307 This agency was established in the Nigerian National Information Technology Development Agency Act 2007.

308 NCAIR website available at ABOUT US – NCAIR (nitda.gov.ng), accessed on 26 February 2024.

309 Supra footnote 274 at 3.

310 WG Evans "Ethics, values and practice" (2019) 74(6) *South African Dental Journal* 333.

311 Libby Bishop "Big data and data sharing: ethical issues" *UK Data Service* (2017) available at https://dam.ukdataservice.ac.uk/media/604711/big-data-and-data-sharing_ethical-issues.pdf, accessed on 7 December 2023.

In this line of reasoning, there are numerous moral values that have been acknowledged as virtues connected to loyalty and honesty by various professional fields. We often tend to minimise the humanitarian component of cybersecurity experts' work. But there is a whole team of experts working to safeguard our personal information, fend off hostile attempts, and handle a variety of security concerns on the opposite side of the screen. The development of ever-newer technologies, such as cloud computing, AI, and the Internet of Things, puts our understanding of what is ethically acceptable and unacceptable in question.[312]

With the rapid development of new technologies, ethical dangers associated to cybersecurity could arise in any aspect of daily life, including healthcare and public safety, and could hurt people to various degrees.[313] Therefore, even though section 32 of the Constitution[314] allows for the "right of access to any information that is required for the exercise or protection of any right and is held by the State or another person", the processing of personal data poses some inherent threats to individual rights,[315] as the data may be misplaced, deleted, subject to an unauthorised alteration, disclosed to third parties, or used in an unlawful manner.[316] Hence, risk management and mitigation depend on the adoption of agreed ethical standards for legal data processing.[317]

Cyber-terrorism, hacking, botnets, and online child exploitations are just a few of the rapidly developing cyberthreats that have given governments an "open invitation" to adopt a "virtual (cyber) turn", investigate, and participate in the virtual border domain diplomatically.[318]

When we talk about AI, we usually mean machines that, given human cognition, judgment, and intent, react to stimuli in a way that is compatible with human behaviour.[319] Their actions are

---

312 Denitsa Kozhuharova, Atanas Kirov and Zhanin Al-Shargabi "Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?" (2022) *Cybersecurity of Digital Service Chains* 203.

313 Janna Anderson and Lee Rainie "Themes: The most harmful or menacing changes in digital life that are likely by 2035" available *at https://www.pewresearch.org/internet/2023/06/21/themes-the-most-harmful-or-menacing-changes-in-digital-life-that-are-likely-by-2035/*, accessed on 07 April 2024.

314 The Constitution of the Republic of South Africa, 1996.

315 Libby Bishop "Big data and data sharing: ethical issues" *UK Data Service*, 2017, available at *https://dam.ukdataservice.ac.uk/media/604711/big-data-and-data-sharing_ethical-issues.pdf*, accessed on 7 December 2023.

316 The Promotion of Access to Information Act 2 of 2000 controls information access and makes it possible for individuals to obtain information owned by both public and commercial entities.

317 Ibid footnote 317.

318 Mark B Manantan "Defining Cyber Diplomacy", available at *https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/*, accessed on 7 December 2023.

319 Willem Gravett "The dark side of Artificial intelligence: Challenges for the Legal System" (2020) 35(1) *University of South Africa Press* 3.

deliberate, wise, and flexible, and in the past few years it has been growing rapidly around the world is quickly changing society and businesses with a variety of opportunities and difficulties,[320] and some of its generative tools, such as ChatGPT, has been used by majority of stakeholders in companies as a means to ease work burdens.

In South Africa, where the AI market is expanding rapidly and is being adopted more and more in the fields like security, healthcare, education, agriculture and corporate, good governance and the management of AI ethics are critical.[321] And with South Africa lacking these in-depth regulatory framework to govern AI which leads to companies that create or use any AI systems exposed to ethical problems and scrutiny from the public, this presents an important question of whether organisations can guarantee the moral, responsible, and reliable use of AI when there are no rules and legislation.[322]

Without a doubt, advancements in robotics and AI have the potential to change people's lives and the way they work, increase productivity, save money, increase safety, and offer better services in the short- to medium-term.[323] While there are numerous economic benefits to the present trend towards creating intelligent, autonomous equipment that can learn and make judgments on their own, there are also a number of social and political issues that are brought up by these machines' potential repercussions on society as a whole.[324]

Ethical problems of AI can also be recognised in technology, value, innovation and regulatory systems. In the four major systems, the basic patterns of ethical problems can become uncontrolled risks, behavioural disorders, and ethical disorders.[325] When choosing the path, AI governance strategies such as ethical embedding, evaluation, adaptation and construction should be implemented within the technology life cycle in the research and development, design and manufacture, experimental funding and deployment and application phases. Looking at the role configuration, multiple actors should assume different roles, including providing ethical factual

---

320 Emile Ormond "Governance of AI Ethics: Perspective from the Global South (Africa)" (2023) *Social Science Research Network* 1 available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4368020*, accessed on 7 December 2023.

321 Willem Gravett "The dark side of Artificial intelligence: Challenges for the Legal System" (2020) 35(1) *University of South Africa Press* 3.

322 Ibid footnote 321 at 3.

323 Ibid footnote 321 at 2.

324 Ibid footnote 321 at 1.

325 Lan Xue and Zhenjing Pang "Ethical governance of artificial intelligence: An integrated analytical framework" (2022) 1 *Journal of Digital Economy* 44.

information, expertise and analysis, as well as expressing ethical feelings or providing ethical regulatory tools under different governance strategies.[326]

4.4 FRAMEWORKS AND PROTOCOLS FOR CYBERATTACKS AND DATA BREACHES

Companies have been vulnerable to data breaches that are caused internally or externally by hackers. A data breach is referred to as a purposeful or accidental release of electronically obtained information by a company, which can contain financial, private, or customer data.[327] Data breaches are frequently viewed as information privacy issues, because of the significant effects that a data breach could have on customers, should their personally identifiable information ("PII") be leaked.[328]

In essence, a data breach at a company might jeopardise information gathered from stakeholders like clients and suppliers as well as vital and non-essential tasks information assets required for the company's operations. In any case, compromising information that is considered important might have detrimental effects on a business. When information belonging to customers along with other third parties becomes compromised because of problems with service failure and breach of trust, it is frequently regarded as more serious.[329]

The era of infallible encryption, secure e-commerce, enjoyable games, real people fighting wars, and the internet being securely managed by reputable companies is long gone. With outdated cybersecurity norms failing, management of the internet has turned into a "free-for-all" and nothing is "hackproof".[330]

A comprehensive analysis of stakeholders, their diverse roles, attitudes, and behaviours has elucidated the numerous contradictions inherent in a multifaceted ecosystem inside a cyber-

---

326 Lan Xue and Zhenjing Pang "Ethical governance of artificial intelligence: An integrated analytical framework" (2022) 1 Journal of Digital Economy 44.

327 Sigi Gooda, Hartmut Hoehle, Viswanath Venkatesh *et al* "User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach" (2017) 41(3) *MIS Quarterly* 704.

328 Mary Culnan and Cynthia Williams "How Ethics Can Enhance Organizational Privacy: Lessons from the Choice point and TJX Data Breaches" (2009) 33(4) *MIS Quarterly* 679.

329 Zareef Mohammed "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches" (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 42.

330 Anthony Minnaar "'Crackers', cyberattacks, and cybersecurity vulnerabilities: The difficulties in combatting the 'new' cybercriminals" (2014) 2 *Acta Criminologica: Southern African Journal of Criminology* 127.

physical society. Lack of action, planning, and policy has been caused by ignorance, a limited comprehension of what is required to be done, and a lack of knowledge of the issue despite its seriousness and necessity.[331] The United States National Institute of Standards and Technology currently outlines a five-step process[332] for avoiding cyberattacks: "identification, protection, detection, response and recovery."[333]

4.4.1 PROTOCOLS FOR REPORTING IN THE EVENT OF CYBERATTACKS AND DATA BREACHES

Because the loss of data is an infringement on the POPIA[334] and may result in criminal or civil charges, section 22 of the Act states that

> "where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the Responsible Party must report this to the Information Regulator, and to the data subject."

This is the protocol for all companies that should be adhered to in order to be compliant with the law and protect its clients and employees. It becomes more difficult to fix weaknesses the longer the breach remains undetected. Affected individuals have a right to know if there is a chance that their data has been hacked and that they can take precautions to lessen the damage, such notifying their bank that their bank information has been exposed.[335] When there is a high likelihood that the breach may cause harm to the data subject's livelihood or reputation, they must be informed.[336]

It is the duty of the individual with knowledge of a breach to report the breach or suspected breach. The individual in question should report as soon as they become aware of the breach, the report may be submitted in writing or verbally and a written account of the incident using the

---

331 Hans de Bruijn and Marijn Janssen "Building cybersecurity awareness: The need for evidence-based framing strategies" (2017) 34 *Government Information Quarterly* 3.

332 The United States National Institute of Standards and Technology "promotes U. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." Available at *https://www.usa.gov/agencies/national-institute-of-standards-and-technology*, accessed on 07 April 2024.

333 The US Cybersecurity Framework is available on Computer Security and Resource Center, available at *https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters*, accessed on 10 February 2024.

334 Protection of Personal Information Act 4 of 2013.

335 The Personal Data Breach Reporting Procedure is available on the African Union Development Agency (AUDA-NEPAD) website, available at *https://www.nepad.org/sites/default/files/resourcefiles/AUDA-NEPAD%20Personal%20Data%20Breaches%20Procedure.pdf*, accessed on 10 February 2024.

336 Ibid footnote 335.

standardised forms created for this purpose must come after an oral submission. Employees who neglect to notify a suspected or confirmed breach will face disciplinary action.[337]

4.4.2 PROTOCOLS FOR RESPONDING IN THE EVENT OF CYBERATTACKS AND DATA BREACHES

The NCPF"[338] of South Africa, which was adopted in 2012, stipulates the creation of a national Information Security Incident Management Capability ("ISIMC"), also known as a national Computer Security Incident Response Team ("CSIRT"), via the National Cybersecurity Hub.[339] The NCPF offers a thorough road map for tackling the nation's cybersecurity issues, with key aspects such as Policy Objectives, Risk Management Approach, Legal and Regulatory Framework, Capacity Building and Awareness, Public-Private Partnerships, Incident Response and Crisis Management, International Cooperation, and Monitoring and Evaluation.[340]

As a result, an incident response team was formed to identify and address cyberattacks that arise, while also providing support to a client or constituency.[341] Incident response teams are becoming more and more required by companies, including vital infrastructure, and are an essential component of incident handling skills. They are highly sought after by corporations for their diverse skill set, particularly in the areas of cyber security and cyber incident management.[342]

In countries, such as the Netherlands, CSIRTs play a vital role for companies when it comes to responding to data breach incidents and effectively managing the occurrence, data loss or theft, and workflow disruptions brought on by incidents.[343] Incident response teams can be structured

---

337 The Personal Data Breach Reporting Procedure is available on the African Union Development Agency (AUDA-NEPAD) website, available at *https://www.nepad.org/sites/default/files/resourcefiles/AUDA-NEPAD%20Personal%20Data%20Breaches%20Procedure.pdf*, accessed on 10 February 2024.

338 The National Cybersecurity Policy Framework is available at *https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf*, accessed on 10 February 2024.

339 Morné Pretorius and Hombakazi Ngejane "Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC)" (2019) 24 *The African Journal of Information and Communication* 2.

340 Hans de Bruijn and Marijn Janssen "Building cybersecurity awareness: The need for evidence-based framing strategies" (2017) 34 *Government Information Quarterly* 2.

341 Ibid footnote 340.

342 Pauline Meyer and Sylvain Métille "Computer security incident response teams: are they legally regulated? The Swiss example" (2022) 4 *International Cybersecurity Law Review* 39.

343 Rick van der Kleij, Geert Kleinhuis and Heather Young "Computer Security Incident Response Team Effectiveness: A Needs Assessment" (2017) 8 *Frontiers in Psychology* 2.

formally, where conducting incident response is their primary role. Alternatively, these teams can also operate in a more ad hoc manner, with members assembled as needed to address incidents.[344]

According to Chen *et al*,[345] it is possible to establish CSIRT so that responding to incidents is their primary duty. These teams can additionally be more flexible in nature, with members assembled only when necessary to address an incident.[346] These employees are typically found in the companies' own IT departments. Upon detection of an incident, someone on the team will have the lead in handling it, contingent on the severity and knowledge of the incident as well as staff availability.[347] In an ideal scenario, the team evaluates the incident data, assesses the occurrence's impact, and takes the necessary action to minimise damage and resume regular operations.[348]

Therefore, in an event of a cyberattack or data breach, companies are expected to have established guidelines and practices in place to deal with such situations and lessen their effects. Usually, these procedures entail identifying the breach, containing the damage to prevent further unauthorised access to company data, the company's security incident response team should promptly organise the response operations and carry out the incident response strategy, and notify various affected parties.

4.4.3 PROTOCOLS FOR RECOVERING IN THE EVENT OF CYBERATTACKS AND DATA BREACHES

A company must determine which stakeholders are impacted by a data breach and how they may impact the company in turn. A company's attempts to recover from a data breach may not succeed if the main stakeholders impacted by the incident are not satisfied.[349]

After the incident is resolved it is advisable for companies to execute a thorough post-incident analysis in order to assess the success of the response efforts, find any holes or weak points in the

---

344 Rick van der Kleij, Geert Kleinhuis and Heather Young "Computer Security Incident Response Team Effectiveness: A Needs Assessment" (2017) 8 Frontiers in Psychology 2.

345 Tiffani Chen, Daniel Shore and Stephen Zaccaro *et al* "An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams" (2014) 12(5) *IEEE Security & Privacy* 61-67.

346 Tiffani Chen, Daniel Shore and Stephen Zaccaro *et al* "An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams" (2014) 12(5) *IEEE Security & Privacy* 66.

347 Ibid footnote 346 at 67.

348 Ibid footnote 346 at 67.

349 Zareef Mohammed "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches" (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 44.

current security controls and incident response protocols, and put the changes that are required into place in order to improve the cybersecurity defences of the company.

The Canadian health information systems sets an example of this after it experienced no less than 14 significant cyberattacks since 2015, 9 of these have tried ransomware, and 6 have resulted in protected health information ("PHI") compromise.[350] Additionally, the attack may result in data breaches, in which patient health information is stolen from health information systems and sold illegally online.[351] Canada learned that provinces and territories ought to create databases of breaches on health information systems that are accessible to the public.[352] Patients may choose to seek out physicians with a solid cybersecurity track record if these repositories are available, which can help study and influence consumer choice.[353]

Any company may experience a data breach, thus it's critical that senior management implement a plan for dealing with these situations. The first step in doing this is figuring out who the key players are who can have a big impact on the company after a data breach. Customers, workers, and regulatory agencies are identified as the primary stakeholders in data breach situations. Nevertheless, additional stakeholders may also have a primary impact on an organisation's success or failure after a data breach. Managers must think about who can have an impact on the company in the event of a data breach and how to handle the concerns they bring up.[354]

While implementing appropriate security and privacy procedures in advance can speed up the procedure and regulatory recovery efforts, it's crucial for a company to be ready to defend its safety and privacy processes to regulatory bodies while strengthening any socio-technical weaknesses that were used in the attack.[355]

---

350 Vinyas Harish, Alun Ackery and Kiran Grant *et al* "Cyberattacks on Canadian health information systems" (2023) 195 (45) *CMAJ* E1548.

351 Vinyas Harish, Alun Ackery and Kiran Grant *et al* "Cyberattacks on Canadian health information systems" (2023) 195 (45) SMAJE1548.

352 Hannah Neprash, Claire McGlave, Dori Cross *et al* "Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021" (2022) 3(12) *JAMA Health Forum* 3

353 Ibid footnote 352.

354 Mary Culnan and Cynthia Williams "How Ethics Can Enhance Organizational Privacy: Lessons from the Choice point and TJX Data Breaches" (2009) 33(4) *MIS Quarterly* 679.

355 Zareef Mohammed "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches" (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 56.

4.5 A DISCUSSION OF THE IMPLICATIONS OF DATA BREACHES ON COMPANIES AND STAKEHOLDERS

The case of *Hawarden vs Edward Nathan Sonnenbergs Inc*[356] ("ENS") highlights the significance of legal practitioners following the generally accepted standard of ethics in the legal profession and honouring their duty of care to clients. In *casu*, the plaintiff had been exchanging emails with a secretary in the conveyancing department of ENS regarding a property that she was buying, ENS was the property seller's representative.[357] The plaintiff was required to electronically transfer a substantial amount of money of R5.5 million into the attorney trust account of the ENS in order to complete the purchase.[358] Regrettably, hackers gained access to the plaintiff's email account. Through the creation of an email address that was identical to the ENS legal secretary's, with the term "africa" substituted with "afirca," fraudsters were able to pass for the ENS legal secretary.[359] The bank account information, purportedly used as ENS's attorney trust account, was contained in a PDF attachment that the hackers sent.[360]

As a result, the plaintiff transferred her debt related to the property into the incorrect bank account. The money had already been taken out of the bank account the cybercriminals had created by the time the error was discovered.[361] Then, the plaintiff asserted that ENS had a responsibility to handle the transaction with appropriate caution, to alert her of the risks associated with Business Email Compromise (or "BEC"), and to securely provide her with the banking information.[362] The plaintiff argued the defendant was responsible to her in negligent for the financial loss she had experienced because ENS had breached this duty of care.[363] The court established that there is a standard for holding legal professionals responsible for carelessness in the performance of their professional obligations.

In this ruling, the court was faced with -

---

356 (13849/2020) [2023] ZAGPJHC 14; [2023] 1 All SA 675 (GJ); 2023 (4) SA 152 (GJ) (16 January 2023).

357 *Hawarden vs Edward Nathan Sonnenbergs Inc* (13849/2020) [2023] ZAGPJHC 14; [2023] 1 All SA 675 (GJ); 2023 (4) SA 152 (GJ) (16 January 2023) at paragraph 2.

358 Ibid footnote 357.

359 Ibid footnote 357 at paragraph 88.

360 Ibid footnote 357.

361 Ibid footnote 357 at paragraph 113.

362 Ibid footnote 357 at paragraph 17.

363 Ibid footnote 357 at paragraph 107.

> "the vexed question of whether or not to impose liability for pure economic loss sustained by the plaintiff who fell victim to cyber-crime through business email compromise ("BEC") as a result of the defendant's negligent omission to forewarn the plaintiff of the known risks of BEC and to take the necessary safety precautions that are designed to safeguard against the risk of harm occasioned by BEC from eventuating."[364]

This decision established new guidelines for how businesses can protect themselves against illegal behaviour on the internet and set a significant precedent for handling.

Equifax, one of the 3 major credit reporting companies in the United States of America ("US"), suffered a significant data breach impacting over 140 million Americans in 2017 that included Social Security numbers, credit card details, email addresses, and numbers from driver's licenses.[365] The company had inadequate information security procedures even prior to the data leak; since 2013, they have been breached annually. In particular, prior to the 2017 data breach, credit reports, customer information, and staff data were all made public despite warnings about potential issues and insufficient security measures.[366]

Even though Equifax discovered and became aware of the breach from July 2017, the executives did not release the data breach information until 7 September 2017, which contributed to the company's image being damaged and customers no longer having faith in them even though they tried several post-breach actions to gain customer's confidence back.[367]

This breach resulted in Equifax to enhance their cybersecurity protocols and to appoint a staff member to administer the cybersecurity program, carry out yearly evaluations of the information security risk, implement controls to thwart cyberattacks, enhance testing and monitoring protocols, and secure independent confirmation of an enhanced cybersecurity program. This requirement is a crucial area of rehabilitation on which Equifax has to concentrate.[368]

Another data breach example that led to huge implications is that of a software development company in the US called Citrix. The business experienced a data breach in 2019 when six

---

364 A discussion of this case was peer reviewed by Juta in Juta and POPIA Portal "What we think about…Hawarden vs Edward Nathan Sonnenbergs Inc" (2023) 17 *Juta & Company Limited* 1.

365 Zareef Mohammed "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches" (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 49.

366 Ibid footnote 365 at 50.

367 Ibid footnote 365 at 49.

368 Ibid footnote 365 at 51.

terabytes of information were stolen by Iranian hackers.[369] About 24,314 people, including workers, contractors, interns, job hopefuls, beneficiaries, and dependents of the business, were impacted by the stolen data.[370]

According to investigations, the hackers utilised a "password spraying" approach, which prevents user lockouts by using the same login for several accounts. Once they gained access to the system, they would work on elevating access to further sensitive data. Emails, company records, confidential internal files, and designs were among the information taken in the data breach.[371]

In accordance with several US data breach reporting laws, Citrix did inform the impacted parties about the data incident, however, Lindsey Howard, former staff member of Citrix, launched sued Citrix. Her lawsuit stated that:

> "The data breach was the inevitable result of Citrix's inadequate approach to data security and the protection of its employees' personal information that it collected during the course of its business."

Because majority of the affected stakeholders, Citrix reached an agreement that compensated the impacted former and current workers of the data breach in the amount of 2.28 million US dollars and further pledged to enhance the information security strategy for a duration of three years.[372]

The difference between the Citrix and Equifax case is that there isn't any concrete proof that Citrix broke any laws that required them to make amends after the data breach. This might be because the data breach case was just resolved, or it could mean that Citrix was already in compliance with the law, but the attack that resulted in the data breach was too strong for the regulations to stop.[373] While regulatory resolution might not be a primary emphasis in this instance, it is nevertheless important for many firms that suffer from breaches of data in general. In essence, data breach incidents might differ in the individuals they impact and incur large expenses for the company.[374]

---

369 Zareef Mohammed "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches" (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 51.

370 Sabina Weston "Citrix employees win $2.3m settlement over 2019 data breach", available at *https://www.itpro.com/security/data-breaches/358454/citrix-employees-win-2*, accessed on 10 February 2024.

371 Ibid footnote 369 at 52.

372 Zareef Mohammed "Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches" (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 52.

373 Ibid footnote 372 at 70.

374 Ibid footnote 372.

4.6 CONCLUSION

In conclusion, the ethical and legal implications of South Africa's privacy and cybersecurity regulations highlight the country's dedication to upholding individual liberties and encouraging appropriate data stewardship in the digital age. A thorough cybersecurity strategy must include frameworks and methods for handling cyberattacks and data breaches, highlighting the significance of proactive risk management and incident response readiness. For the benefit of all of its citizens, South Africa could improve its cybersecurity resilience, protect privacy rights, and promote trust in the digital world by skilfully establishing the complicated convergence of law, ethics, and technology.

Integrating foreign studies can offer valuable insights and lessons for South African companies. By examining how other countries have tackled similar cybersecurity challenges, South Africa can gain a broader perspective on effective strategies, technologies, and policies. Foreign examples can provide practical guidance on mitigating cyber threats, enhancing infrastructure resilience, and implementing robust data protection measures. Additionally, analysing international incidents and responses can help anticipate emerging threats and develop proactive defence mechanisms. Ultimately, leveraging foreign studies allows South Africa to benefit from the collective knowledge and experiences of the global cybersecurity community, contributing to more informed decision-making and a stronger national cybersecurity posture.

CHAPTER FIVE: RECOMMENDATIONS AND CONCLUSION

This dissertation has explored the intricate legal and ethical challenges surrounding cybersecurity governance in South Africa, particularly in relation to corporate responsibility and protection against cybercrimes. Through an analysis of relevant laws, case studies, and regulatory frameworks, several key findings were identified, providing insights into how South African companies can navigate the growing threat of cyberattacks and data breaches.

5.1 SUMMARY OF FINDINGS

The research confirmed that cybersecurity has become an integral component of corporate governance, driven by the increasing frequency and sophistication of cyberthreats. Companies must address cybersecurity not only as a technical concern but also as a critical aspect of their legal and ethical obligations. The analysis of the Cybercrimes Act and POPIA emphasised that legal compliance is essential for mitigating risks and protecting against cybercrimes. Specifically, businesses are required to report cybercrimes, safeguard critical data, and collaborate with the Information Regulator. However, the gap in clearly defined technical standards within POPIA remains a significant challenge, leaving companies uncertain about what constitutes "reasonable security measures.

Additionally, the dissertation found that South African companies are increasingly required to align their cybersecurity frameworks with both privacy laws and corporate governance frameworks, such as those outlined in the King IV Report on Corporate Governance. These frameworks underscore the importance of board-level oversight in managing cybersecurity risks, ensuring that companies approach cybersecurity governance holistically and in compliance with evolving regulations.

5.2 RESEARCH QUESTIONS ANSWERED

The primary research question “What legislation governs cybersecurity in South Africa and does it provide enough legal protection for companies against cybercrimes and security breaches?” was answered by examining the Cybercrimes Act and POPIA, which provide a foundation for legal protection. However, the study revealed that while these laws are a step in the right direction, they leave certain areas, such as technical security measures, ambiguously defined.

The secondary research questions were also addressed:
a) How do companies ensure alignment between their cybersecurity frameworks and privacy laws? This was explored by showing how businesses must integrate POPIA and other regulations with their internal cybersecurity practices, ensuring they adhere to legal standards.
b) How do companies cultivate awareness of cybersecurity among all stakeholders? The dissertation found that fostering a culture of cybersecurity awareness at all levels of the organisation is critical. Companies must make cybersecurity everyone’s responsibility through regular training and clear communication.

5.3 CONCLUSION AND RECOMMENDATIONS

As cyber threats continue to evolve, companies must not only comply with legal obligations but also integrate cybersecurity deeply into their governance structures. To address the gaps identified in this research, the following recommendations are made:

1. Compliance with the Cybercrimes Act, Data Protection and Privacy: Ensure all cybersecurity measures comply with the Cybercrimes Act, which mandates reporting of cybercrimes, protection of critical data, and cooperation with law enforcement agencies. And, align the company’s cybersecurity policies with POPIA to safeguard personal data and respect privacy rights.

2. Corporate Governance: Incorporate cybersecurity into the company’s corporate governance framework, as recommended by the King IV Report, ensuring that the board of directors oversees cybersecurity strategies and risk management.

3. Comprehensive Cybersecurity strategy: Develop a detailed plan that includes risk assessments, the implementation of robust security controls (such as firewalls, encryption, and multi-factor authentication), and a well-defined incident response plan to handle breaches swiftly and effectively.

4. Cybersecurity Awareness and Accountability: Foster a culture of cybersecurity awareness and accountability throughout the company where cybersecurity is everyone's responsibility. And implement regular training programs and awareness campaigns to keep employees informed about the latest threats and best practices.

5. Regular Cybersecurity Assessments: Schedule frequent assessments and audits to identify and address vulnerabilities. Use these assessments to update security measures continually and ensure compliance with current standards.

6. Collaboration and Information Sharing: Engage with government bodies, industry partners, and cybersecurity experts to exchange information on threats and defences. Participate in forums and joint exercises to improve collective cybersecurity resilience.

7. Embrace Emerging Technologies: Integrate AI, machine learning, and blockchain technologies to enhance your cybersecurity infrastructure. These technologies can help in early threat detection, predictive analysis, and secure data transactions.

In conclusion, this dissertation underscores the importance of addressing the legal and ethical implications of cybersecurity within corporate governance, particularly in an increasingly digital world. Companies must navigate the evolving regulatory landscape to protect against cybercrimes and ensure compliance while fostering a culture of security and ethical responsibility across all levels of the organisation.

BIBLIOGRAPHY

PRIMARY SOURCES

CONSTITUTION

The Constitution of the Republic of South Africa, 1996

LEGISLATION

South African

Child Justice Act 75 of 2008

Companies Act 61 of 1973

Companies Act 71 of 2008

Companies Amendment Act 16 of 2024

Correctional Services Act 111 of 1998

Criminal Law Amendment Act 105 of 1997

Criminal Law (Sexual Offences and Related Crimes) Amendment Act 32 of 2007

Criminal Procedure Act 51 of 1977

Cybercrimes Act 19 of 2020

Electronic Communications and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Financial Intelligence Centre Act 38 of 2001

National Prosecuting Authority Act 32 of 1998

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Regulation of Inception of Communications and Provisions of Communications Related Information Act 70 of 2002

South African Police Services Act 68 of 1995

Foreign

Nigerian National Information Technology Development Agency Act 2007

CASE LAW

South African

Buchler v Minister of SAPS N.O. and Others (6310/2022) [2023] ZAFSHC 1 (5 January 2023)

Cyberscene Ltd v i-Kiosk Internet and Information (Pty) Ltd 2000 3 SA 806 (C)

Goqwana v Minister of Safety NO and Others 2016 (1) SACR 384 (SCA)

Hawarden v Edward Nathan Sonnenbergs Inc (13849/2020) [2023] ZAGPJHC 14; [2023] 1 All SA 675 (GJ); 2023 (4) SA 152 (GJ) (16 January 2023)

Ntozini v S (CA&R 05/2020) [2020] ZAECGHC 104 (15 September 2020)

Okundu v S (CA&R117/16) [2016] ZAECGHC 131 (22 November 2016)

R v Douvenga (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2002, unreported)

Salzmann v S (755/18) [2019] ZASCA 145; [2020] 1 All SA 361 (SCA); 2020 (2) SACR 200

(SCA) (13 November 2019)

Foreign

Rockwell Graphic Systems, Inc. v DEV Industries, Inc., 925 F.2d 174 (1991)

United States v Morris 728 F. Supp. 95 (1990)

SECONDARY SOURCES

BOOKS

Christoph Bartneck and Christoph Lutge "What is ethics" in Christoph Bartneck, *et al* (eds) *An Introduction to Ethics in Robotics and AI* (2021) 17-26

Caroline Ncube, Desmond Oriakhogba, Tobias Schonwetter *et al* "Setting out the challenges and opportunities of artificial intelligence for Africa" in Caroline Ncube, *et al* (eds) *Artificial Intelligence and the Law in Africa* (2023) 1-20

JOURNAL ARTICLES

Adele Thomas "Media-reported corporate governance transgressions in broad-based black economic empowerment deals in the South African mining sector" (2014) 8(2) *African Journal of Business Ethics* 89

Aderinola Dunmade, Adeyinka Tella and Uloma Onuoha "Cyberethics awareness and implications on Library and Information Science educators in selected Universities in South-West Nigeria" (2023) 89(1) *South African Journal of Libraries and Information Science* 1-10

Alok Mishra, Yehia Alzoubi, Memoona Anwar, *et al* "Attributes impacting cybersecurity policy development: An evidence from seven nations" (2022) *Computers & Security* 1-23

Anil Lamba, Satinderjeet Singh, Balvinder Singh *et al* "Analyzing and fixing Cyber Security Threats for Supply Chain Management" (2017) 4(5) *International Journal for Technological Research in Engineering* 5678-5681.

Annalise Kempen "Are we making progress in the fight against cybercrime?" (2016) *Servamus* 19-21

Anne Kohnke and Dan Schoemaker "Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control" (2015) 52:3 *Taylor & Francis* 9-17

Anthony Minnaar "'Crackers', cyberattacks, and cybersecurity vulnerabilities: The difficulties in combatting the 'new' cybercriminals" (2014) 2 *Acta Criminologica: Southern African Journal of Criminology* 127-144

Arti Aneja "Philosophy of Corporate Social Responsibility Vis-à-vis Corporate Governance" (2015) 6(7) *International Research Journal of Management Sociology & Humanity* 155-170

Banuka De Silva "Exploring the Relationship between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review" (2023) 12(1) *International Journal of Information Security and Cybercrime* 23-29

Brett van Niekerk "An analysis of cyber-Incidents in South Africa" (2017) 20 *The African Journal of Information and Communication* 113-132.

Carol Silaule, Lean Makhubele, Stevens Mamorobela "A model to reduce insider cybersecurity threats in a South African telecommunications company" (2022) *South African Journal of Information Management* 1-8

Chiji Ezeji, Adewale Olutola, and Paul Bello "Cyber-related crime in South Africa: Extent and perspectives of state's roleplayers" (2018) 31(3) *Acta Criminologica: Southern African Journal of Criminology* 93-110

Christo Makridis "Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018" (2021) *Journal of Cybersecurity* 1-8

Collins Ntim, Kwaku Opong, Jo Danbolt "The Relative Value Relevance of Shareholder versus Stakeholder Corporate Governance Disclosure Policy Reforms in South Africa" (2012) 20(1) *Corporate Governance: An International Review* 84-105

Cornelius Kilian "A practical explanation of ethics as a good corporate governance principle in South Africa and New Zealand – A case study" (2020) 85(1) *Koers Journal* 1-10

Dawid Szutowski and Piotr Ratajczak “The relation between CSR and Innovation. Model approach” (2016) 12(2) *Journal of Entrepreneurship, Management and Innovation* 77 – 94

Deepansh Kumar, Yugansh Khera, Nidhi Garg, *et al* “Towards the impact of hacking on cyber security” (2018) 9(2) *IIOAB Journal* 61-77

Denitsa Kozhuharova, Atanas Kirov and Zhanin Al-Shargabi “Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?” (2022) *Cybersecurity of Digital Service Chains* 202-221

Emiles Mbungu Kala “The Impact of Cyber Security on Business: How to Protect Your Business” (2023) 13(2) *Open Journal of Safety Science and Technology* 51-65

Eugene Spafford “The Internet Worm Program: An Analysis” (1988) *Purdue Technical Report CSD-1R-823* 1-26

Ewan Sutherland “Governance of Cybersecurity – the case of South Africa” (2017) 20 *The African Journal of Information and Communication* 83-112

Frank Cremer, Barry Sheehan, Michael Fortmann, *et al* “Cyber risk and cybersecurity: a systematic review of data availability” (2022) 47 *The Geneva Papers on Risk and Insurance – Issues and Practice* 698-736

Frederick Lemieux “Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives” (2011) *Developing Cyber Security Synergy* 1

Georgina Broni and John Velentzas “Corporate governance, control and individualism as a definition of business success. The idea of a "post - heroic" leadership” (2012) 1 *Procedia Economics and Finance* 61-70

Gousia Habib, Sparsh Sharma, and Sara Ibrahim *et al* “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing” (2022) 14 *Future Internet* 1-22

Hans de Bruijn and Marijn Janssen “Building cybersecurity awareness: The need for evidence-based framing strategies” (2017) 34 *Government Information Quarterly* 1-7

Hannah Neprash, Claire McGlave, Dori Cross *et al* “Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021” (2022) 3(12) *JAMA Health Forum* 1-11

Hamid Tohidi and Mohammad Jabbari “The important of Innovation and its Crucial Role in Growth, Survival an organisations” (2011) *Elsevier Ltd* 535-538

Heloise Pieterse “The Cyber Threat Landscape in South Africa: A 10-Year Review” (2021) 28 *The African Journal of Information and Communication* 1-21

Jeffrey Proudfoot, Ryan Schuetzler, Justin Giboney, et al “Trends in Phishing Attacks: Suggestions for Future Research” (2011) 25 *Information Systems and Quantitative Analysis Faculty Proceedings & Presentations* 1-8

Isabel Maria Lopes, Teresa Guarda and Pedro Oliveira “Implementation of ISO 27001 Standards as GDPR Compliance Facilitator” (2019) 4(2) *Journal of Information Systems Engineering & Management* 3

Joel Chigada and Rujeko Madzinga “Cyberattacks and threats during COVID-19: A systematic literature Review” (2021) 23(1) *South African Journal of Information Management* 1-11

Juta and POPIA Portal “What we think about…Hawarden vs Edward Nathan Sonnenbergs Inc” (2023) 17 *Juta & Company Limited* 1-3

Kamshad Mohsin “Data Privacy and Cybersecurity” (2022) *SSRN* 1-6

Lan Xue and Zhenjing Pang “Ethical governance of artificial intelligence: An integrated analytical framework” (2022) *Journal of Digital Economy* 44-52

Lubna Dhirani, Noorain Mukhtiar, Bhawani Chowdhry, *et al* “Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review” (2023) 23(3) *Sensors* 1-8

Manuel Alfonso Garzón Castrillón “The concept of corporate governance” (2021) 25(2) *Revista Científica "Visión de Futuro"* 177-190

Mary Culnan and Cynthia Williams “How Ethics Can Enhance Organizational Privacy: Lessons from the Choice point and TJX Data Breaches” (2009) 33(4) *MIS Quarterly* 673-687

Michael Haenlein and Andreas Kaplan "A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence" (2019) 61(4) *California Management Review* 1-10.

Mikhail Shlyakhtunov "White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies" (2021) 12(8) *International Journal of Advanced Computer Science and Applications* 429-435

Min Xu, Jeanne David and Suk Kim "The Fourth Industrial Revolution: Opportunities and Challenges" (2018) 9(2) *International Journal of Financial Research* 90-95

Myles Garvey "A Philosophical Examination on the Definition of Cyberspace" (2021) *Cyber Security and Supply Chain Management* 1-11

Monray Botha "The Role and Duties of Directors in the promotion of Corporate Governance: A South African perspective" (2009) *Obiter* 702-715

Morné Pretorius and Hombakazi Ngejane "Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC)" (2019) 24 *The African Journal of Information and Communication* 1-20

Muhammad Safitra, Muharman Lubis and Hanif Fakhrurroja "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity" (2023) 15 *Sustainability* 1-32

Munish Sharma "Data Theft: Implications for Economic and National Security" (2017) 11(1) *Journal of Defence Studies* 61-80

N Mans-Kemp, P Erasmus and S Viviers "Advances in the corporate governance practices of

Johannesburg Stock Exchange companies" (2016) 20 *Southern African Business Review* 71-93

Nabeelah Daniels and Anna-Retha Smit "Corporate governance and the value relevance of accounting information: Empirical evidence from South Africa" (2023) 25 *Southern African Journal of Accountability and Auditing Research* 21-36

Nereida Hadziahmetovic, Nejla Salihovic "The Role of Transparent Communication and Leadership in Employee Engagement" (2022) 11(2) *International Journal of Academic Research in Economic & Management Sciences* 561

Nnenna Ifeanyi-Ajufo "Cyber governance in Africa: at the crossroads of politics, sovereignty and

Cooperation" (2024) 6(2) *Policy design and practice* 146-159

Oladotun E Awosusi "The imperative of Cyber Diplomacy and Cybersecurity in Africa: A new means to a Borderless Regional End?" (2022) 9(3) *Journal of African Foreign Affairs* 71

Oluwatoyin Akinbowale, Heinz Klingelhofer, Mulatu Zerihun, *et al* "Development of a policy and regulatory framework for mitigating cyber fraud in the South African banking industry" (2024) 10 *Heliyon* 1-17

Pauline Meyer and Sylvain Métille "Computer security incident response teams: are they legally regulated? The Swiss example" (2022) 4 *International Cybersecurity Law Review* 39-60

Pieter Bezuidenhout "An IT auditor's view of a hacker's methodology" (2005) 2005(22) *Auditing SA* 25-26

Prasdika Prasdika and Bambang Sugiantoro "A review paper on Big Data and Data Mining concepts and techniques" (2018) 7(1) *International Journal on Informatics for Development* 33-35

Prashant Khanpara and Vivek Prasad "Honeypot: A way to capture attackers" (2023) *International Journal of Novel Research and Development* 1-5

Rick van der Kleij, Geert Kleinhuis and Heather Young "Computer Security Incident Response Team Effectiveness: A Needs Assessment" (2017) 8 *Frontiers in Psychology* 1-8

Scott Timcke, Mark Gaffley and Andrew Rens "The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet" (2023) *The African Journal of Information and Communication* 1-28

Serkan Savas and Suleyman Karatas "Cyber governance studies in ensuring cybersecurity: an overview of Cybersecurity governance" (2022) 3 *International Cybersecurity Law Review* 14

Shivanshi Sinha and Yojna Arora "Ethical hacking: The story of a white hat hacker" (2020) 8(3) *International Journal of Innovative Research in Computer Science & Technology* 131-136

Sigi Gooda, Hartmut Hoehle, Viswanath Venkatesh *et al* "User compensation as a data breach recovery action: an investigation of the Sony PlayStation network breach" (2017) 41(3) *MIS Quarterly* 704-727

Sizwe Snail "Cybercrime in South Africa – Hacking, cracking, and other unlawful online activities' (2009) 1 *Journal of Information, Law & Technology* 1-23

Sizwe Snail ka Mtuze and Melody Musoni "An overview of cybercrime law in South Africa" (2023) 4 *International Cybersecurity Law Review* 299-323

Tiffani Chen, Daniel Shore and Stephen Zaccaro et al "An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams" (2014) 12(5) *IEEE Security & Privacy* 61-67

Uchenna Jerome Orji "The African Union Convention: A regional response towards cyber stability*?" (2018) 12(2*) *Masaryk University Journal of Law and Technology* 91-129

Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, *et al* "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review" (2023) 23 (4117) *Sensors* 1-46

Vinyas Harish, Alun Ackery and Kiran Grant *et al* "Cyberattacks on Canadian health information systems" (2023) 195 (45) *CMAJ* E1548-E1554

Werner Schoeman "Corporate Governance – Less is More" (2022) 36(2) *Speculum Juris* 411-425
WG Evans "Ethics, values and practice" (2019) 74(6) *South African Dental Journal* 333-334

Willem Gravett "The dark side of Artificial intelligence: Challenges for the Legal System" (2020) 35(1) *University of South Africa Press* 2

Włodzimierz Sroka and Marketa Lőrinczy "The perception of ethics in business: analysis of research Results" (2015) 34 Procedia Economics and Finance 156-163

Yonnique Hanusch "Financial institutions should decline hackers' requests for voluntary compensation" 2021) 40(2) *South African Journal of Philosophy* 162-170

Zareef Mohammed “Data breach recovery areas: an exploration of organization’s recovery strategies for surviving data breaches” (2021) *Organizational Cybersecurity Journal: Practice, Process and People* 41-59

Zibin Zheng, Shaoan Xie and Hongning Dai *et al* “An overview of Blockchain Technology: Architecture, Consensus, and Future trends” (2017) *IEEE* 557-564

DISSERTATIONS AND THESES

Lindokuhle Ramalepe *Ethical Corporate Governance: The significance and impact of ethics in the South African Corporate Culture* (Unpublished Master’s Degree in Governance and Political thesis, University of The Free State, 2021) 95

INTERNET REFERENCES

Absa Group Limited Integrated Report 2021, available at *https://www.absa.africa/wp-content/uploads/2022/09/Absa-Group-Integrated-Report.pdf*, accessed on 29 April 2024

African Union Cyber Security and Protection of Personal Data Convention available *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*, accessed on 25 January 2024

African Union Development Agency (AUDA-NEPAD) website, available at *https://www.nepad.org/sites/default/files/resourcefiles/AUDANEPAD%20Personal%20Data%20Breaches%20Procedure.pdf*, accessed on 04 February 2024

Alfonso Arellano and Noelia Camara “The importance of ICT in society’s needs: An empirical approach Through Maslow’s lens”, available at *https://www.researchgate.net/publication/343788818_The_importance_of_ICT_in_society's_needs_An_empirical_approach_through_Maslow's_lens*, accessed on 11 December 2023

Allison Job “Did one simple issue crash Liberty?”, available at *https://www.itweb.co.za/article/did-one-simple-issue-crash-liberty/dgp45qaGabl7X9l8*, accessed on 29 April 2024

Andre Barrinha and Thomas Renard "Cyber-diplomacy: the making of an international society in the Digital age" (2017) 3 *Global affairs* at 353, available at *https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924*

Bart Lenaerts-Bergmans "What is spoofing attacks?", available at *https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/*, accessed on 19 December 2023

Business Tech "South Africa under cyberattack: Interpol reveals top threats in South Africa", available at *https://businesstech.co.za/news/it-services/531990/south-africa-under-cyber-attack-interpol-reveals-top-threats-in-south-africa/*, accessed on 7 December 2023

Centre for AI Research available at *https://www.cair.org.za/about*, accessed on 07 April 2024

Center for Scientific and Industrial Research available at *https://www.csir.co.za/*, accessed on 07 April 2024

Computer Security and Resource Center "Cybersecurity Framework", available at *https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters*, accessed on 10 February 2024

Council of Europe "Convention on Cybercrime", available at *https://www.coe.int/en/web/cybercrime/the-budapest-convention*, accessed on 30 November 2023

Council of Europe "South Africa Cybercrime policies/strategies", available at *https://www.coe.int/en/web/octopus//southafrica#:~:text=The%20Government%20of%20South%20Africa,19%20of%202020*, accessed on 30 November 2023

Discovery "Governance Report for the year ended 30 June 2023", available at *https://www.discovery.co.za/assets/discoverycoza/corporate/investor-relations/2023/discovery-governance-report.pdf*, accessed on 29 April 2024

Discovery “POPIA: Protection of Personal Information Act”, available at *https://www.discovery.co.za/corporate/popia-security*, accessed on 29 April 2024

Elmarie Kritzinger, “Online safety in South Africa - A cause for growing concern" *2014 Information Security for South Africa*, Johannesburg, South Africa, 2014, available at *https://ieeexplore.ieee.org/document/6950502*, accessed on 30 November 2023

Emile Ormond “Governance of AI Ethics: Perspective from the Global South (Africa)” (2023) *Social Science Research Network* 1-23 available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4368020*, accessed on 7 December 2023

European Union General Data Protection Regulation, available at *https://gdpr-info.eu/*, accessed on 29 January 2025

Financial Sector Conduct Authority available at *https://www.fsca.co.za/Documents/FSCA_Strategy_2018.pdf*, accessed on 25 April 2024

ImmuniWeb “South Africa POPIA Compliance and Cybersecurity”, available at *https://www.immuniweb.com/compliance/popia-compliance-privacy-cybersecurity/*, accessed on 29 November 2023

Information Regulator website available at *https://registrations.inforegulator.org.za/landing*, accessed on 07 April 2023

Interpol “Interpol report identifies top cyberthreats in Africa” available at *https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa*, accessed on 7 December 2023

Institute of Directors Southern Africa “General Guidance note: Board composition”, available at *https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/49D62EF3-F749-403C-BE47-73C50F27F30F/General_Guidance_Note_on_Board_Composition.pdf*, accessed on 25 April 2025

Institute of Directors Southern Africa “King IV report on corporate governance for South Africa 2016”, *available at https://www.adams.africa/wp-content/uploads/2016/11/King-IV-Report.pdf,* accessed on 20 November 2023

Janna Anderson and Lee Rainie “Themes: The most harmful or menacing changes in digital life that are likely by 2035” available at *https://www.pewresearch.org/internet/2023/06/21/themes-the-most-harmful-or-menacing-changes-in-digital-life-that-are-likely-by-2035/,* accessed on 07 April 2024

Joe Warminsky “South Africa credit bureau breached, data reportedly held for $15M ransom”, available at *https://cyberscoop.com/south-africa-transunion-data-breach/,* accessed on 29 April 2024

John Campbell “Last Month, Over Half-a-Billion Africans Accessed the Internet”, available at *https://www.cfr.org/blog/last-month-over-half-billion-africans-accessed-internet,* accessed on 12 May 2024

JSE corporate governance framework, available at *https://group.jse.co.za/governance/corporate-governance-framework,* accessed on 25 April 2025

Karen Allen “South Africa lays down the law on cybersecurity”, available at *https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime,* accessed on 30 November 2023

Kristyna Svobodova “POPI Act: The scope, purpose, and how to comply”, available at *https://www.safetica.com/blog/popi-act-the-scope-purpose-and-how-to-comply*, accessed on 02 April 2024

Lexis Nexis “JSE Limited Listings Requirements”, available at *https://www.jse.co.za/sites/default/files/media/documents/201904/JSE%20Listings%20Requirements.pdf,* accessed on 27 January 2025

Libby Bishop “Big data and data sharing: ethical issues” *UK Data Service*, 2017, available at *https://dam.ukdataservice.ac.uk/media/604711/big-data-and-data-sharing_ethical-issues.pdf,* accessed on 7 December 2023

Makoma Toona “How the South African Cybercrimes Act 19 of 2020 will affect individuals and Businesses”, available at *https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses*, accessed on 30 November 2023

Mark B Manantan “Defining Cyber Diplomacy”, available at *https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/*, accessed on 7 December 2023

Michael Mncedisi Willie “The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture” available at

https://www.researchgate.net/publication/371399113_The_Role_of_Organizational_Culture_in_Cybersecurity_Building_a_Security-First_Culture, accessed on 04 February 2024

Michalsons “Cybercrime Act in South Africa | Overview and Read”, available at *https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world/cybercrimes-act-southafrica#:~:text=The%20Cybercrimes%20Act%20gives%20the%20Police%20Service%20(and%20their%20members,they%20have%20a%20search%20warrant*, accessed on 24 November 2023

National Cybersecurity Policy Framework is available at *https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf*, accessed on 04 February 2024

NCAIR available at *ABOUT US – NCAIR (nitda.gov.ng)*, accessed on 26 February 2024

Nnenna Ifeanyi-Ajufo “Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation”, *https://www.tandfonline.com/doi/full/10.1080/25741292.2023.2199960*, accessed on 30 November 2023

OECD, available at *https://www.oecd.org/countries/nigeria/*, accessed on 26 February 2024.

Parmi Natesan and Prieur du Plessis "Corporate Governance: South Africa's secret weapon", available at *https://www.iodsa.co.za/news/538251/Corporate-governance-South-Africas-secret-weapon.htm*, accessed on 24 February 2024

PR de Wet and David Olen "South Africa: The Cybercrimes Act, its relation with POPIA, and Compliance", available at *https://www.dataguidance.com/opinion/south-africa-cybercrimes-act-its-relationship%C2%A0-popia*, accessed on 30 November 2023

Proofpoint "What is Phishing?", available at *https://www.proofpoint.com/us/threat-reference/phishing*, accessed on 19 December 2023

PwC South Africa "King IV – Steering point", available at *https://www.pwc.co.za/en/publications/king4.html*, accessed on 24 April 2024

Redscan "Breach and Attack Simulation", available at *https://www.redscan.com/services/breach-andattacksimulation/#:~:text=A%20breach%20and%20attack%20simulation%20is%20a%20type%20of%20advanced,be%20used%20by%20malicious%20actors*, accessed on 12 December 2023

Ridwaan Boda and Naledi Ramoabi "Data security breach: Information Regulator takes action against Department of Justice" available at *ENS - News - Data security breach: Information Regulator takes action against Department of Justice (ensafrica.com)*, accessed on 08 February 2024

Riskonnect "RMIS: The definitive guide", available at *https://riskonnect.com/resources/rmis-the-definitive-guide/*, accessed on 27 January 2025

R Nidumolu, CK Prahalad and MR Rangaswami "Why Sustainability Is Now the Key Driver of Innovation", available at *https://hbr.org/2009/09/why-sustainability-is-now-the-key-driver-of-innovation*, accessed on 24 February 2024

Sabina Weston “Citrix employees win $2.3m settlement over 2019 data breach”, available at *https://www.itpro.com/security/data-breaches/358454/citrix-employees-win-2*, accessed on 10 February 2024

Sasol Limited sustainability report, available at *https://www.sasol.com/investor-centre/sustainability-reporting*, accessed on 29 April 2024

South African Reserve Bank available at *https://www.resbank.co.za/en/home/what-we-do/Prudentialregulation/governance-structures*, accessed on 25 April 2024

Tashreek Miller “Mitigate the Risk – Cybersecurity in South Africa”, available at *https://fwblaw.co.za/mitigate-the-risk-cybersecurity-in-south-africa/*, accessed on 29 November 2023

TechTarget “Malware”, available at *https://www.techtarget.com/searchsecurity/definition/malware#:~:text=Malware%2C%20or%20malicious*, accessed on 19 December 2023

United States National Institute of Standards and Technology available at *https://www.usa.gov/agencies/national-institute-of-standards-and-technology*, accessed on 07 April 2024

Webber Wentzel “The liability of directors in cyberspace”, available at *https://qa.webberwentzel.com/News/Pages/the-liability-of-directors-in-cyberspace.aspx*, accessed on 25 January 2024

Woolworths Holdings Limited “Governance report 2022”, available at *https://www.woolworthsholdings.co.za/wpcontent/uploads/2022/09/Governance_Report_2022.pdf*, accessed on 29 April 2024

World Bank “Cyber threats to the financial sector in Africa”, available at

https://documents1.worldbank.org/curated/en/099830405172214598/pdf/P16477000601530760af01093740e385fe8.pdf, accessed on 07 April 2024

World Economic Forum "Nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat. What can they do about it?", available at *https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/*, accessed on 06 April 2024.