

https://dspace.org/

Cybersecurity Risks in Automation Technologies for the Future of Work in South Africa's Digital Banking Sector

Adewunmi, Olawunmi

2025
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/49190
Adewunmi, Olawunmi . (2024). Cybersecurity Risks in Automation Technologies for the Future of Work in South Africa's Digital Banking Sector [Masters dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/49190

Downloaded from a DSpace repository. https://dspace.org/

Cybersecurity Risks in Automation Technologies for the Future of Work in South Africa's Digital Banking Sector.

Olawunmi Adewunmi

2721656

2721656@students.wits.ac.za

+2349036833664

A research project submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Supervised by Professor Colin Chibaya

Johannesburg, 2025

ABSTRACT

The rapid adoption of automation technologies is transforming South Africa's digital banking sector, enhancing efficiency and customer experience. However, this digital transformation introduces significant cybersecurity risks that threaten financial institutions, customers, and regulatory frameworks. This study investigated the cybersecurity risks associated with automation technologies in digital banking and their implications for the future of work. Grounded in the NIST Risk Management Framework and ISO 27005, the research employed a qualitative methodology, gathering data through semi-structured interviews with IT managers in digital banks. The findings highlighted key cybersecurity threats, including phishing, malware, ransomware, and insider attacks, exacerbated by automation technologies. Additionally, the study revealed that digital transformation is widening the cybersecurity skills gap, necessitating targeted upskilling initiatives.

To mitigate these risks, South Africa's digital banking industry must adopt proactive cybersecurity measures, invest in workforce training, and implement robust risk management frameworks. The study concluded that while automation technologies offer immense potential, their secure integration is critical for the resilience and sustainability of the banking sector in the digital age.

KEYWORDS

Automation Technologies

Cybersecurity Risks

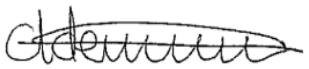
Digital Banking

Digital Transformation

Future of Work

DECLARATION

I, _____Olawunmi Adewunmi_____, declare that this research report is my work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the Master of Management degree in Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Olawunmi Adewunmi Signature: 

Signed at …Johannesburg, South Africa……

On the ……28th…….. day of February…… 2025.

DEDICATION

To my beloved family: my mother, Lady Teniade Adewunmi; my siblings Yewande, Adebolatan, and Ayodeji, with their spouses, Joshua, Tutu, and Tope; my nieces, Adora and Dara; and my nephews, David and Asher. This research project is a tribute to each of you. Your belief in me made me who I am. As I take this step forward, I know your presence is forever linked to my accomplishments.

ACKNOWLEDGEMENTS

I am grateful to my supervisor, Prof Colin Chibaya, for his support, advice and assistance throughout this research. I would also like to thank my sister, Prof. Yewande Adewunmi Abolarinwa, for her encouragement and help in paying my tuition fees and for her financial assistance in providing accommodation to me as an international student. I am indebted to the Wits Business School family, particularly the Faculty of Commerce, Law and Management family, for their support and assistance. Finally, I would say a big thank you to God for his continual provision and support in every way.

TABLE OF CONTENTS

LIST OF TABLES……xii
LIST OF FIGURES……..xii
LIST OF ACRONYMS……xiii
CHAPTER 1. INTRODUCTION……..1
1.1 STATEMENT OF PURPOSE…….. 2
1.2 BACKGROUND OF THE STUDY 3
1.3 RESEARCH PROBLEM 5
1.4 RESEARCH QUESTIONS.....7
1.5 RATIONALE.....7
1.6 DELIMITATIONS OF THE STUDY.....8
1.7 DEFINITION OF TERMS……11
1.8 ASSUMPTIONS……14

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK ……16
2.1 INTRODUCTION 16
2.2 DEFINITION OF TOPIC OR BACKGROUND DISCUSSION 17
2.3 CYBERSECURITY THREATS POSED BY AUTOMATION TECHNOLOGIES OF THE FUTURE OF WORK IN DIGITAL BANKING 18
2.3.1 CYBERSECURITY THREATS RESULTING FROM RELIANCE ON AUTOMATION TECHNOLOGIES…… 18
2.3.2 CYBERSECURITY THREATS IMPACT THE WORKFORCE AND THE SKILLS GAP……..19
2.3.3 CYBERSECURITY RISKS IN DIGITAL BANKING AND ITS REGULATORY CHALLENGES . ……..19
2.3.4 PROPOSITION 1……..20
2.4 HOW THE SOUTH AFRICA'S DIGITAL BANKING INDUSTRY MITIGATES THE CYBERSECURITY ATTACK RISK IDENTIFIED BY AUTOMATION TECHNOLOGIES 21
2.4.1 DIGITAL BANKING IS FACED WITH CYBERSECURITY THREATS DUE TO AUTOMATION TECHNOLOGIES…….. 21
2.4.2 CONNECTION BETWEEN AUTOMATION TECHNOLOGIES AND THE EMERGENCE OF NEW CYBERSECURITY RISKS..... 24
2.4.3 HOW AUTOMATION TECHNOLOGIES MIGHT RESHAPE THE CYBERSECURITY LANDSCAPE IN SOUTH AFRICA'S DIGITAL BANKING 24

2.4.4 Proposition 2……...25
2.5 IDENTIFYING HOW THE RAPID ADOPTION OF DIGITAL BANKING AUTOMATION TECHNOLOGIES IMPACTS THE SKILLS GAP IN CYBERSECURITY PROFESSIONALS…….. 26
2.5.1 RAPID ADOPTION OF DIGITAL BANKING AUTOMATION TECHNOLOGIES. 26

2.5.2 FUTURE OF WORK IN SOUTH AFRICA.....26
2.5.3 IMPACT ON SKILLS GAP IN CYBERSECURITY PROFESSIONALS.....27
2.5.4 Proposition 3 29
2.6 ANALYTICAL FRAMEWORK.....29
2.6.1 THEORETICAL FRAMEWORK..... 29
2.6.2 CONCEPTUAL FRAMEWORK..... 33
2.7 CONCLUSION OF LITERATURE REVIEW.....34

CHAPTER 3. RESEARCH METHODOLOGY.....35
3.1 RESEARCH PARADIGM.....35
3.2 RESEARCH APPROACH.....36
3.3 RESEARCH DESIGN.....37
3.4 DATA COLLECTION METHODS.....37
3.5 POPULATION AND SAMPLE.....37
3.5.1 POPULATION..... 38
3.5.2 SAMPLE AND SAMPLING METHOD..... 38
3.6 THE RESEARCH INSTRUMENT.....39
3.7 PROCEDURE FOR DATA COLLECTION.....39
3.8 DATA ANALYSIS STRATEGIES AND INTERPRETATION.....39
3.9 POSSIBLE LIMITATIONS AND CHALLENGES OF THE STUDY.....43
3.10 QUALITY ASSURANCE.....44
3.10.1 TRANSFERABILITY..... 44
3.10.2 DEPENDABILITY..... 44
3.10.3 CREDIBILITY..... 45
3.10.4 CONFIRMABILITY.....45
3.11 ETHICAL CONSIDERATIONS.....46

CHAPTER 4. PRESENTATION OF FINDINGS.....47
4.1 Introduction..... 47
4.2 Overview of the study..... 47
4.3 Findings of Proposition 1..... 48
4.3.1 Data Analysis of Proposition 1… 48
4.3.2 Proposition 1..... 50
4.3.2.1 Area..... 51
4.3.2.1.1 Participant 1..... 51
4.3.2.1.2 Participant 2..... 51
4.3.2.1.3 Participant 3..... 52
4.3.2.1.4 Participant 4..... 52
4.3.2.1.5 Participant 5..... 52
4.3.2.1.6 Participant 6..... 52
4.3.2.1.7 Participant 7..... 53

4.3.2.1.8 Participant 8…… 53
4.3.2.1.9 Participant 9…… 54
4.3.2.1.10 Participant 10…… 54
4.3.2.2 Vulnerability…….. 55
4.3.2.2.1 Participant 1…….. 56
4.3.2.2.2 Participant 2……. 56
4.3.2.2.3 Participant 3…….. 56
4.3.2.2.4 Participant 4……. 56
4.3.2.2.5 Participant 5……. 57
4.3.2.2.6 Participant 6……. 57
4.3.2.2.7 Participant 7……. 57
4.3.2.2.8 Participant 8…….. 58
4.3.2.2.9 Participant 9…….. 58
4.3.2.2.10 Participant 10…… 59
4.3.2.3 Exploit…… 60
4.3.2.3.1 Participant 1…….. 60
4.3.2.3.2 Participant 2…….. 61
4.3.2.3.3 Participant 3…….. 61
4.3.2.3.4 Participant 4…….. 61
4.3.2.3.5 Participant 5……. 61
4.3.2.3.6 Participant 6……. 62
4.3.2.3.7 Participant 7…… …… 62
4.3.2.3.8 Participant 8…… 63
4.3.2.3.9 Participant 9……. 63
4.3.2.3.10 Participant 10…….. 63
4.3.3 Conclusion of Proposition 1……. 64
4.4 Findings of Proposition 2…….. 65
4.4.1 Data Analysis for Proposition 2…… 65
4.4.2 Proposition 2…… 66
4.4.2.1 Organisation…….. 67
4.4.2.1.1 Participant 1…….. 68
4.4.2.1.2 Participant 4…….. 68
4.4.2.1.3 Participant 5…….. 68
4.4.2.1.4 Participant 7…….. 69

4.4.2.1.5 Participant 8……. 69
4.4.2.1.6 Participant 9……. 70
4.4.2.2 Regulation……. 70
4.4.2.2.1 Participant 1……. 70
4.4.2.2.2 Participant 5……. 70
4.4.2.2.3 Participant 8…… 71
4.4.2.3 Technology……... 71
4.4.2.3.1 Participant 1…….. 72
4.4.2.3.2 Participant 2……. 72
4.4.2.3.3 Participant 3…….. 73
4.4.2.3.4 Participant 4…….. 74
4.4.2.3.5 Participant 5…….. 74
4.4.2.3.6 Participant 6…….. 75
4.4.2.3.7 Participant 7…….. 75
4.4.2.3.8 Participant 8…….. 76
4.4.2.3.9 Participant 9……. 77
4.4.2.3.10 Participant 10……... 77
4.4.3 Conclusion of Proposition 2……... 79
4.5 Findings of Proposition 3…….. 79
4.5.1 Data Analysis of Proposition 3……..... 79
4.5.2 Proposition 3…….. 81
4.5.2.1 Skills……... 82
4.5.2.1.1 Participant 1…….. 83
4.5.2.1.2 Participant 2…….. 83
4.5.2.1.3 Participant 3……. 83
4.5.2.1.4 Participant 4…….. 83
4.5.2.1.5 Participant 5…… 83
4.5.2.1.6 Participant 6…… 84
4.5.2.1.7 Participant 7…… 85
4.5.2.1.8 Participant 8…… 85
4.5.2.1.9 Participant 9…… 86
4.5.2.1.10 Participant 10……. 86
4.5.2.2 Education…… 87
4.5.2.2.1 Participant 1…… 87

4.5.2.2.2 Participant 2…… 88
4.5.2.2.3 Participant 3…… 89
4.5.2.2.4 Participant 4……. 89
4.5.2.2.5 Participant 5……. 89
4.5.2.2.6 Participant 6……. 90
4.5.2.2.7 Participant 7……..…. 91
4.5.2.2.8 Participant 8……..…. 93
4.5.2.2.9 Participant 9……..……. 94
4.5.2.2.10 Participant 10……..…….. 94
4.5.3 Conclusion of Proposition 3……..…….. 96
4.6 Summary of the findings…….. 96

CHAPTER 5.DISCUSSION OF THE FINDINGS…… 97
5.1 Introduction……. 97
5.2 Demographic profile of respondents……..…… 97
5.3 Discussion on Proposition 1……..…….. 101
5.3.1 Discussion on Interview Question 1……. 101
5.3.2 Discussion on Interview Question 2……. 103
5.3.3 Discussion on Interview Question 3…..…… 105
5.4 Discussion on Proposition 2……..……. 107
5.4.1 Discussion on Interview Question 4……. 107
5.4.2 Discussion on Interview Question 5……. 109
5.5 Discussion on Proposition 3…….. 110
5.5.1 Discussion on Interview Question 6…… 111
5.5.2 Discussion on Interview Question 7…… 112
5.5.3 Discussion on Interview Question 8……. 114
5.6 Conclusion……. 116

CHAPTER 6 CONCLUSIONS & RECOMMENDATIONS…… …….. 118
6.1 Introduction…… . 118
6.2 Conclusions Regarding Research Question 1…….. 119
6.3 Conclusions Regarding Research Question 2……... 120
6.4 Conclusions Regarding Research Question 3…… 120
6.5 Recommendations……. 121

6.6 Contributions…… 122
6.7 Suggestions for further research…….. 123

REFERENCES ……125
APPENDIX A
(Tables)……168
Table 1A: Theme-Category Codebook of Theme 1……..168
Table 2A: Category-Code Codebook of Theme ……170
Table 3A: Theme-Category Codebook of Theme 2…… ..173
Table 4A: Category-Codes Codebook of Theme 2…… .175
Table 5A: Theme-Category Codebook of Theme 3…… .178
Table 6A: Category-Code Codebook of Theme 3…… .179
Table 7A: Comparison of theoretical expectations and findings in Prop 1….180
Table 8A: Comparison of theoretical expectations and findings in Prop 2….181
Table 9A: Comparison of theoretical expectations and findings in Prop 3….182

APPENDIX B
(Figures)……...184
Figure 1A: Bar chart graph of Theme 1…… 184
Figure 2A: Word frequencies of Theme 1…… 185
Figure 3A: Network of Theme 1 with the categories and codes…… 186
Figure 4A: Bar chart graph of Theme 2…… 187
Figure 5A: Word frequencies of Theme 2…… 188
Figure 6A: Network showing Theme 2 with the categories and codes… .. 189
Figure 7A: Bar chart graph of Theme 3…… 190
Figure 8A: Word frequencies of Theme 3…… 191
Figure 9A: Network of Theme 3 with the categories and codes……. 192

APPENDIX C (Interview Guide)..…… 193
APPENDIX D (Consent form)…..…… 194
APPENDIX E (Participant Information Sheet)……..…… 195

LIST OF TABLES

Table 2.1: Ways of mitigating cybersecurity risks in digital banks.....13
Table 3.2: Consistency table: research questions, propositions, data collection and data analysis…… 41
Table 4.3: Interview Questions of Theme 1…… 48
Table 4.4: Interview Schedule as per Theme 1…… 48
Table 4.5: Theme 1 showing categories with the number of quotations……50
Table 4.6: Interview Questions of Theme 2……65
Table 4.7: Interview Schedule as per Theme 2…… 65
Table 4.8: Theme 2 shows categories and each number of quotations…... 67
Table 4.9: Interview Questions about Theme 3…..…… 80
Table 4.10: Interview Schedule as per Theme 3…….. 80
Table 4.11: Theme 3 with each category and number of quotations…… 82
Table 5.12: Demography profile of respondents…… 97
Table 5.13: Categories-Code Codebook of demographics profile of respondents. 98

LIST OF FIGURES

Figure 1.1: Conceptual Framework…….....3
Figure 5.2: Demographics of respondents' profiles of participants' nationalities across the three Themes……99

Figure 5.3: Demographics of respondent profiles on participant genders across the three Themes……..…… 100
Figure 5.4: Demographics of respondents' profiles on participants' degrees across the three Themes…… 100

LIST OF ACRONYMS

ABBREVIATION	DESCRIPTION
AI	Artificial Intelligence
AT	Automation Technologies
CR	Cybersecurity Risks
ML	Machine Learning
RPA	Robotic Process Automation
UEBA	User and Entity Behaviour Analytics

CHAPTER 1. INTRODUCTION

Automation technologies can replace human workers with technology (Nof, 2009). They can create a harmonious co-existence between humans and technology in a sustainable society and natural environment (Tzafestas, 2010). The primary aim of automation technologies is to provide a human-centric approach in the banking industry, enabling it to gain competitive advantages (Tzafestas, 2010). Automation technologies are pivotal in transforming traditional banking services into digital banking (Jana et al., 2021). This transformation allows customers to access banking products and services through electronic or online platforms (Jana et al., 2021).

Banks' digital transformation emphasises the enhancement of digital channels while acknowledging the continued importance of physical channels for specific needs (Baskerville et al., 2020). The core of this digital transformation in the banking industry is the integration of automation technologies and systems such as blockchains and big data (Campino et al., 2021). Blockchain technology harnesses advanced record-keeping methods and has potent applications (Lee and Armstrong, 2023). It possesses advantages over traditional databases, such as decentralisation, security, and shareability (Lee and Armstrong, 2023). On the other hand, big data is characterised by high volume, velocity, variety, and veracity (data accuracy) (Lee and Armstrong, 2023). It serves as a critical driving force of the Fourth Industrial Revolution, enabling significant progress in what digital banks can accomplish with data and fueling the growth of artificial intelligence (Lee and Armstrong, 2023). Together, these technologies and systems bring about the future of work.

Cybersecurity risk refers to the likelihood of a socio-technical system being compromised or failing (Cains et al., 2022). Such risks depend on several factors, such as human behaviour or physical vulnerabilities in the system (Cains et al., 2022). These factors commonly impact control, prioritisation of resources, and system functionality (Cains et al., 2022). Consequently, system integrity, confidentiality, and availability are compromised (Jung et al., 2001).

Cybersecurity risks are introduced by the increased adoption of automation technologies in South Africa's digital banking sector (Masheleni, 2022). These demand robust security measures to protect sensitive financial information and maintain customer trust (Olaiya et al., 2024).

The future of Work is a crucial concern. It primarily concerns the impact of automation technology development on job availability, income inequality, precarious work situations, remote work, and the recruitment of qualified individuals (Santana and Cobo, 2020). This study explores the concept of digital banking, examining the current trends in the banking industry in South Africa. On the other hand, digital transformation reflects endeavours towards the use of automation technologies in the banking industry in South Africa. Consequently, the concept of automation technologies brings the 'how' aspect of the digital transformation process on board. Thus, the idea of the future of work closes the story, depicting aspects related to when such digital transformation would be effected. This study assesses future cybersecurity risks in automation technologies for the digital banking sector in South Africa.

1.1. Statement of purpose

The explicit statement of the study's purpose implies a focus on the practicality and convenience of the future of work in the digital banking sector in South Africa, which involves identifying cybersecurity risks associated with automation technologies in the industry.

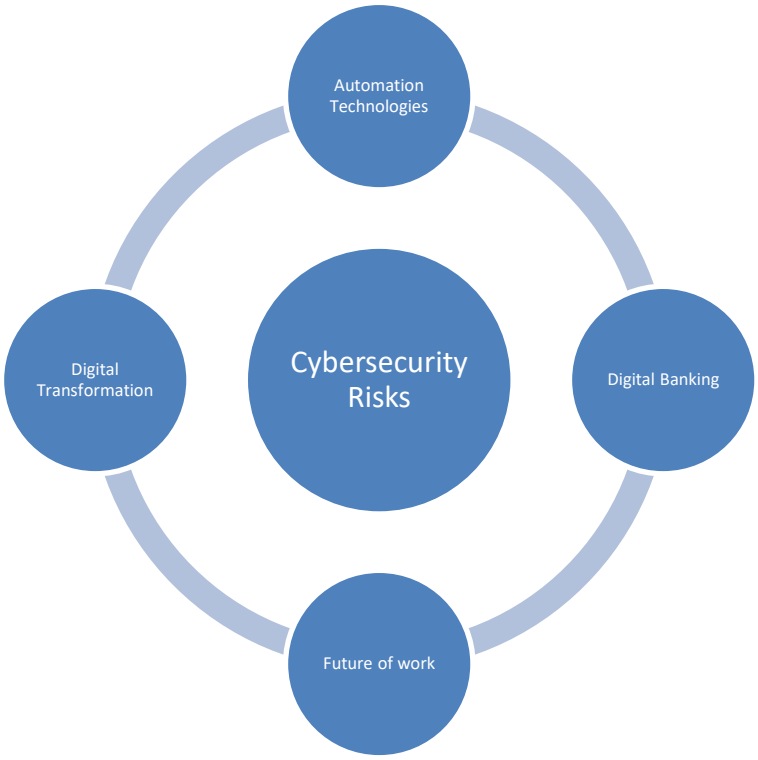


Figure 1.1: Conceptual Framework

To support the inquiry, the researcher drew insight from the invaluable experience of the respondents, who were sampled from practitioners in the information technology cognate disciplines and the banking sector.

1.2 Background of the study

With its unique digital banking landscape, South Africa initially connected to the Internet in 1996 (Maniraj Singh, 2004). Digital banking services were introduced in 2000 (Borg and Persson, 2010). By March 2009, over five million South Africans had adopted digital banking, with more than three million actively using it (Dagada, 2013). These figures depict an impressive expansion and triumph of automation technologies in the digital banking sector, as well as their remarkable resilience and ability to thrive despite the cybersecurity risks expressed by users and banking regulators (Dagada, 2013). The population of digital banking users in South Africa exceeded one million by the conclusion of 2003 (Lewis, 2005). It increased to 1.4 million in 2004 and reached 1.7 million in 2005 (Barnard and Moolman, 2008). Following 2005, there was a noticeable increase in digital bank accounts (Dagada, 2013), insinuating a promising future

and the apparent survival and thriving of the digital banking sector (Dagada, 2013).

With the advent of the Fourth Industrial Revolution, staying up-to-date has never been more critical. Various industries, including the banking sector, are rapidly shifting or strengthening their business models and services to digital platforms (Louw and Nieuwenhuizen, 2020). Traditional banks in South Africa are at the forefront of this digital transformation, adapting, strengthening and thriving. The banks now provide e-customers with a wide range of services, including user-friendly websites (Louw and Nieuwenhuizen, 2020), digital banking capabilities, and access to the Internet through dedicated Operating Systems and Android apps. They also provide locally zero-rated data for using these apps, allowing Unstructured Supplementary Service Data options for digital banking and point-of-sale systems. This diverse service portfolio, tailored to the evolving needs of their customers, highlights these institutions' adaptability and unwavering customer-centric approach, which instils confidence in the industry's future (Louw and Nieuwenhuizen, 2020).

Before the emergence of digital banks, Absa Bank, Nedbank, Standard Bank, and First National Bank wielded considerable power in the country's banking industry (Tshabalala, 2021). Their competitive edge stemmed from incorporating Industry 4.0 technology into their core functions, enabling them to offer tailored services and cost-effective options (Tshabalala, 2021). Nevertheless, their supremacy diminished after numerous small and medium-sized banking sectors transitioned to digital platforms (Tshabalala, 2021).

The emergence of digital-only banks challenged traditional business models (Nel and Boshoff, 2021). Fortunately, some customers of conventional banks remained hesitant to switch to digital-only banks because they were satisfied with their current situation. Thus, their reluctance to open accounts with digital-only banks may stem from their preference for traditional banks, shaped by their current satisfaction with the problem (Nel and Boshoff, 2021).

Nonetheless, even the traditional South African banks eventually considered transitioning significantly from a conventional setup to a digital one in the

postmodern era (Koenaite et al., 2021). This shift to digital banking is not an isolated event, but rather part of the global wave associated with the Fourth Industrial Revolution. The fourth industrial revolution seeks to transform industries worldwide, including banking (Koenaite et al., 2021). In South Africa, this transformation is particularly pronounced, with the exponential expansion of online banking being a direct consequence of incorporating advanced automation technologies into every facet of our daily lives, a product of the Fourth Industrial Revolution (Mujinga, 2024).

Like many other nations, South Africa is experiencing a surge in digital banking adoption (Adeleye et al., 2024). The convenience and accessibility offered by digital platforms have made them increasingly popular among consumers (Amat-Lefort and Barnes, 2024). Nevertheless, the country has also witnessed a growing number of cybersecurity attacks targeting financial institutions, highlighting the urgent need for robust cybersecurity measures (Mphahlele, 2024). The intersection of automation technologies, digital banking, and cybersecurity forms the core of this research. By examining the cybersecurity risks associated with automation technologies in the South African digital banking landscape, this study aims to contribute to the development of effective strategies to mitigate these threats. Understanding the vulnerabilities and challenges the South African banking industry faces is crucial for developing tailored solutions. The future of work is undergoing a significant transformation due to automation technologies (William et al., 2023). As more tasks are automated, the role of human employees will evolve, requiring new skills and competencies (Morandini et al., 2023). This research examines the impact of automation technologies on the workforce within the banking sector, identifying potential cybersecurity risks associated with changes in job roles and responsibilities.

1.3. Research Problem

This study's research problem is cybersecurity risks associated with adopting automation technologies in the future of work threaten stakeholders, especially in the digital banking industry in South Africa. Key concerns stem from the increasing reliance on digital systems and the evolving sophistication of

cybersecurity attacks (Thakur, 2024). Cybersecurity risks impact many entities, including employees, customers, suppliers, investors, competitors, and governments. These risks may include infrastructure disruptions, national security threats, and economic instability (Kumar, 2023). The consequences of cybersecurity incidents are far-reaching and can have severe repercussions, including direct monetary losses through theft, fraud, or ransom demands (Sharif and Mohammed, 2022). Also, stakeholders may suffer reputational damages resulting in loss of customer trust, decreased market share, and negative publicity (Perera et al., 2022). In addition, cybersecurity incidents may bring about operational disruptions, leading to system downtime, data loss, and business interruptions (Ibiyemi and Olutimehin, 2024). Legal liabilities may also emanate, such as lawsuits, fines, and regulatory penalties (Nash, 2021). Threats such as espionage, sabotage, and infrastructure attacks (Patel and Chudasama, 2021) would be apparent.

Numerous studies have examined cybersecurity risks, focusing on various aspects such as threat landscape analysis and identifying emerging threats and vulnerabilities (Gajjar and Taherdoost, 2024). Risk assessment methodologies have been proposed that focus on developing frameworks for evaluating cybersecurity risks (Hubbard and Seiersen, 2023). Other frameworks emphasised incident response and recovery, suggesting strategies for mitigating the impact of cybersecurity attacks (Staves et al., 2022). However, compelling studies examining cybersecurity governance and management focused on organisational structures and processes for managing cybersecurity (Shah et al., 2022). However, despite this extensive research, several gaps persist, including gaps related to a focus on technical aspects (Catal et al., 2023). Many studies focus on technical vulnerabilities and solutions, neglecting human factors and organisational behaviour (Catal et al., 2023). There is an apparent limited understanding of emerging threats because of technology's rapid evolution out-paces research, leaving gaps in knowledge about new attack vectors (Axon et al., 2022). There is also an evident lack of comprehensive risk assessment frameworks. Existing frameworks often overlook specific industry sectors or emerging technologies (Imran et al., 2022). More so, there is insufficient attention to human-centred security, where the role

of human error and social engineering in cybersecurity attacks remains understudied (Grobler et al., 2021).

The research gap lies in the need for a comprehensive study that analyses the specific cybersecurity threats targeting automation technologies for digital banks in South Africa. There is a lack of studies assessing the effectiveness of current cybersecurity measures implemented by digital banks in identifying the root causes of vulnerabilities in the South African digital banking ecosystem. This study seeks to propose tailored cybersecurity strategies to mitigate risks and enhance reliance in the South African banking sector. Therefore, the problem statement addressed in this research study contributes precisely to developing more effective cybersecurity strategies for mitigating cybersecurity risks associated with digital transformation in the banking industry.

1.4. Research questions.

This study seeks to respond to the following three research questions in succession:

1. What are the cybersecurity threats posed by automation technologies of the future of work in digital banking?

2. How can the South African digital banking industry mitigate the cybersecurity risks identified from bringing on board automation technologies for the future of work in the banking sector?

3. How does identifying cybersecurity risks associated with digital banking automation technologies in the future of work in South Africa impact the skills gap in cybersecurity professionals?

1.5 Rationale

Cele and Kwenda's (2024) study examines long-term solutions for cybersecurity challenges in the banking sector, which this study will also investigate. This study aims to build upon Cele and Kwenda's (2024) work by exploring the transformative potential of integrating automation technologies into the digital

banking landscape. This study also examines the unique cybersecurity threats that may emerge from automation technologies in the future of digital banking. Completing these tasks is an ambitious but self-fulfilling journey.

This study aims to shed light on how the swift adoption of digital banking automation technologies in the future of work in South Africa will impact the cybersecurity skills gap. Such information will be of value to all stakeholders, but mainly to cybersecurity professionals and banks. Thus, the implications of this study have immediate known beneficiaries. Contributing insights that would inspire known beneficiaries around our communities would be a worthwhile milestone.

Additionally, the findings of this study impact the lives of many others. The researcher's qualifications will be enhanced, and the same research will contribute to the body of knowledge. Other researchers to follow will benefit from the insights shared in this study. Hopefully, citing part of the work would put the researcher on the map, which would be a compelling achievement.

In addition, undertaking this study in digital banking is not just an academic exercise but also a potential solution to the digital banking problem in South Africa. The benefits yielded from the study could be far-reaching, including financial asset protection, global recognition, halting financial crime, enhanced data privacy and customer trust, technological innovation and advancement, and economic stability (Lee, 2021). Involvement in such a journey is a genuine agenda and a compelling rationale for undertaking this study.

1.6 Delimitations of the study

This study is limited to South Africa. South Africa presents a compelling case for studying cybersecurity risks associated with automation technologies in digital banking, given its unique position as Africa's most advanced digital economy and its rapidly transforming financial services sector (Koenaite et al., 2021; Tshabalala, 2021). Over the past two decades, South Africa has seen a significant shift from traditional banking to digital platforms, with major banks such as Absa, Nedbank, Standard Bank, First National Bank and FirstRand

Bank investing heavily in automation technologies and AI technologies to enhance operational efficiency and customer experience (Koenaite et al., 2021; Tshabalala, 2021). The country also faces growing cybersecurity threats, with a noticeable increase in phishing, malware, ransomware, and insider attacks targeting financial institutions (Mphahlele, 2024). This makes the intersection of automation technologies and cybersecurity a timely and critical area of study. Furthermore, South Africa's complex regulatory environment, skills shortages in cybersecurity, and its emerging fintech sector create a highly dynamic landscape for digital banking, unlike more mature or developing economies.

The reason why the banking sector was chosen in this study given that threats are universal for the following reasons. High-Value Target and Systemic Importance: Banks hold liquid assets and vast stores of personally identifiable information; a successful breach therefore yields direct financial gain for attackers and can destabilise public confidence and the broader economy (Taavitsainen, 2025). Because the sector underpins payment, lending and savings functions, even a single significant incident can create knock-on effects for other industries and regulators (Busch, 2024). Rapid and Deep Digital Transformation in South Africa: The user base continued to expand, growing from 1 million in 2003 to 1.7 million in 2005, demonstrating a mature, tech-savvy customer population that is now deeply dependent on online services (Garane, 2024). Established banks (Absa, Nedbank, Standard Bank, FNB) and a wave of digital-only challengers are aggressively deploying AI, robotic process automation, and big data analytics to remain competitive. This makes the sector an ideal natural laboratory for studying automation-driven cyber-risk (Garane, 2024). Demonstrably Rising Threat Level: South African financial institutions have experienced a marked surge in phishing, malware, ransomware and insider attacks over the last decade, highlighting an urgent need for sector-specific defences (Calder and Watkins, 2024).

The combination of large attack surfaces (mobile apps, open-banking APIs, cloud cores) and lucrative pay-offs means banks are constantly at the top of hackers’ target lists (Calder and Watkins, 2024). Dense Regulatory Environment: The sector is simultaneously guided by global standards (e.g.,

Basel III cyber guidance) and local statutes such as POPIA and the SARB's directive on cyber-resilience (Karakasilioti, 2024). Exploring cybersecurity within banking, therefore, sheds light on how organisations juggle compliance, innovation, and risk, with insights readily transferable to other highly regulated domains (Hassan et al., 2024). Socio-Economic Leverage and Generalisability: Banking contributes roughly 20% of South African GDP and is a major employer; securing it protects jobs, savings, and foreign investment (Adjasi and Yu, 2021). Lessons learnt cascade outward: payments, insurance, telecoms, and retail all plug into banking infrastructure, so stronger banking cybersecurity uplifts the entire digital ecosystem (George, 2024). Identified Research Gap: Prior studies have highlighted a lack of granular research on automation technologies and specific cyber threats within South African banks, particularly regarding human factors and skills shortages. Focusing on the sector, therefore, fills a clearly defined scholarly and practical void.

The South African digital banking sector is a dynamic and rapidly evolving landscape, shaped by a unique blend of established traditional banks, agile digital-only entrants, and a complex regulatory environment (Garane, 2024). This organisational context presents both significant opportunities for financial inclusion and innovation, as well as distinct challenges related to infrastructure, consumer behaviour, and evolving risk management (Bello, 2024). Digitised incumbents: Major traditional banks, such as FNB, Nedbank, Standard Bank, Absa, and FirstRand Bank, have heavily invested in digital transformation strategies (Mkele, 2024). Challenger Banks/Neo-banks: These are digital-first banks that operate without physical branches, leveraging mobile apps and web platforms. These are TymeBank, Discovery Bank and Bank Zero (Sibeko, 2023).

This study aims to identify cybersecurity threats to automation technologies and the future of work in the digital banking industry in South Africa. We restrict the scope of our research to literature scoped from the year 2021 to the year 2025. Digital banking, which leverages automation technology in financial services, is a specific area of interest (Oladele, 2024). We aim to gain a precise understanding of the integration of automation technologies for a prosperous

future of work in the banking sector. The study is limited to the context of South African banks. Participants in this study were information technology managers in the banking industry and the labour department in South Africa. We employed a qualitative research approach, based on data collected through interviews with participants. The study primarily includes participants' experiences, supported by data from other sources, such as archives, journals, and textbooks.

1.7. Definition of terms

- In the context of this work, automation technologies automate repetitive processes using actual or virtual robots (Mohammad and Surya, 2018). They encompass a range of tools and systems designed to streamline operations, improve efficiency, and enhance customer experience (Haleem et al., 2021). One of the automation technologies considered in the banking industry is robotic process automation, which uses software robots to automate repetitive, rule-based tasks such as data entry, transaction processing, and compliance reporting (Madakam et al., 2019). This helps reduce errors, increase speed, and free up human employees for more complex tasks (Chugh et al., 2022). Artificial Intelligence and Machine Learning algorithms are also used to analyse vast amounts of data to provide insights, detect fraud, personalise customer services, and optimise credit scoring (Saxena et al., 2023; Patel, 2023). Chatbots and virtual assistants powered by artificial intelligence can handle customer inquiries and provide 24/7 support (Lee, 2020). Also, blockchain technology can enhance the security and transparency of transactions (Kshetri, N. (2021). It is used for secure, tamper-proof record-keeping, cross-border payments, and smart contracts (Sanka et al., 2021). Customer Relationship Management Systems can also manage customer interactions, track customer data, and provide personalised marketing and service recommendations based on customer behaviour and preferences. (Anshari et al., 2019). Automation technologies enable banks to improve operational efficiency, reduce costs, enhance security, and deliver a better customer experience (Jaiwant, 2022).

- Cybersecurity Risk is defined as the likelihood that a sociotechnical system will be harmed or fail, depending on several known and unknown

factors, including human behaviour, an individual's perception of risk, and physical and cybersecurity vulnerabilities in the system that impact control, prioritisation of resources, and system functionality (Cains et al., 2022). Various threats can compromise the integrity, confidentiality, and availability of banking systems and customer data (Jung et al., 2001). Key risks include phishing and social engineering, where attackers may use deceptive emails, messages, or phone calls to trick employees or customers into revealing sensitive information such as login credentials or account details (Lee and Armstrong, 2023). It also includes malware and ransomware, where malicious software can infect banking systems, leading to data breaches, unauthorised access, or encryption of critical data (Lee and Armstrong, 2023). Ransomware can lock banks out of their systems, demanding payment for restoration (Lee and Armstrong, 2023). Employees or contractors with access to banking systems may intentionally or unintentionally compromise security, leading to data leaks, fraud, or sabotage (Achor, 2023). Attackers can flood banking websites or services with excessive traffic, causing disruptions and making it difficult for legitimate users to access their accounts (Aslan et al., 2023). Also, unauthorised access to sensitive customer data, such as personal information, account details, and transaction histories, can lead to identity theft, financial fraud, and loss of customer trust (Cassim, 2015). In addition, banks often rely on third-party vendors for various services (Bronson, 2022). Weak security practices among these vendors can create vulnerabilities that attackers can exploit. (Bronson, 2022). Similarly, the growing use of Internet of Things (IoT) devices in banking (such as intelligent ATMs) introduces new attack vectors if these devices are not adequately secured (Ahvanooey et al., 2021). This could be coupled with cloud security issues, including data breaches, misconfigurations, and unauthorised access (Loureiro, 2021).

- Digital banking incorporates technology into every aspect of financial services operations (Sanmath, 2019). This transformation involves using digital platforms and technologies to offer banking services over the Internet, enabling customers to manage their finances, conduct transactions, and access banking services through computers, smartphones, and other digital devices (Lottu et al., 2023). Critical aspects of digital banking include online banking, mobile

banking, digital wallets and payment systems, ATM services, electronic funds transfer, personal finance management tools that help customers track their spending, budget, and manage their finances more effectively, chatbots, virtual assistants, and other AI-driven tools to provide customer support and answer queries (Hakizimana et al., 2023).

- Digital Transformation in the banking industry is defined as the sector's current major transition towards digitalisation, leading to a fundamental overhaul of the banking system (Omarini, 2017). This transition offers new opportunities for banks to involve customers in the industry's evolution (Omarini, 2017). Emerging technologies seem ready to revolutionise and permanently reconfigure the value chain of financial services (Omarini, 2017). Whether adjusting to change to remain competitive or introducing a new initiative, a bank's digital transformation is significant (Khanboubi and Boulmakoul, 2019).

- The future of work is a projection of the changes that work, labour, and the workplace will undergo in the following years (SHRM, 2023). Shaping the future of work involves crucial elements such as attracting new talent, fostering effective leadership, and building a competitive organisation (Morgan, 2014). The future of work is being shaped by several key trends and developments, primarily driven by technological advancements, changing customer expectations, regulatory changes, and the need for greater efficiency and innovation (West, 2018). Banks need to increase the automation technologies of routine tasks and processes (Jaiwant, 2022). They must continue to invest in digital channels, such as mobile apps and online banking platforms, to provide seamless and personalised customer experiences (Jaiwant, 2022). For example, the COVID-19 pandemic accelerated the adoption of remote work, enabling employees to work from home or other remote locations while maintaining a presence in the office (Barath and Schmidt, 2022). Collaboration tools and virtual meeting platforms will continue to grow, enabling efficient teamwork and communication across different locations (Geyer et al., 2001). As technology evolves, the demand for skills such as data analytics, cybersecurity, AI, and digital marketing is expected to increase (Johnson et al., 2021). Banks must invest in continuous learning and

development programs to equip their workforce with these new skills (Chovarda, 2021). Similarly, employees will be encouraged to learn to stay relevant and competitive in a rapidly changing industry, advancing data analytics to gain insights into customer behaviour, optimise operations, and make informed business decisions (Davenport et al., 2010). This will leverage customer data to offer personalised products and services, enhancing customer satisfaction and loyalty, increasingly offering products and services that support environmental sustainability, such as green bonds and sustainable investment funds (Alhawamdeh et al., 2024).

1.8. Assumptions

The following assumptions were made:

1. This study examined South Africa's evolving cybersecurity laws and other new regulations enacted within the banking industry of South Africa. When completing this study, the new rules and regulations override any standing rules.

2. The digital banking sector widely believes that job cuts will result from the adoption of automation technologies. Although some roles may no longer be required after automation, there is potential for creating a new scope of positions in the industry. We assume that the implications of any job cuts will be offset by the new positions that will arise.

3. This study highlights the changing nature of cybersecurity risks. Cybercriminals will use new tactics to exploit weaknesses in automated systems. We assume that new automation technologies possess features to counter perpetrators' efforts.

4. This study investigates the necessity for bank employees to receive comprehensive training in identifying and responding to cybersecurity threats within an automated environment. We assume such training resources are available for a smooth transition.

5. The managers interviewed are competent to provide the correct information for the research.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

The literature review is a critical examination of academic articles relevant to a research study. This literature review reflects on works related to the following questions:

1. What are the cybersecurity threats posed by automation technologies of the future of work in digital banking? In response to this question, we agree that cybersecurity threats posed by automation of the future of work in digital banking include phishing attacks (Alkhalil et al., 2021; Jain and Gupta, 2022; Basit et al., 2021); password attacks (Guan and Chen, 2022; Islam et al., 2023), insider attacks (Daubner et al., 2023; Abulencia, 2021), social engineering attacks (Syafitri et al., 2022; Fuertes et al., 2022), malware attacks (Selvaganapathy et al., 2021; Roseline and Geetha, 2021), ransomware attacks (Reshmi, 2021; Kara and Aydos, 2022) and Distributed-Denial-of-Service (DDOS) attacks (Lee and Armstrong, 2023; Mittal et al., 2023). This study also examines evolving cybersecurity attacks and breaches in physical security, which the researchers fail to consider.

2. How can the South African digital banking industry mitigate the cybersecurity risk identified from bringing on board automation technologies for the future of work in the banking sector? In this question, this study also agrees with the South African digital banking industry's way of mitigating the risk of cybersecurity attacks identified above through the following: hiring skilled cybersecurity staff (Crumpler and Lewis, 2022; Jordan, 2022), staff training (Dash and Ansari, 2022; Okafor et al., 2023), digital identity (Binhammad et al., 2024; Chakraborty et al., 2023), collaboration (Polis, 2023; Jimmy, 2021), dealing with work-from-home (Dai et al., 2023; Pranggono and Arabo, 2021), cutting-edge cybersecurity software (Shwedeh et al., 2023; Lee and Armstrong, 2023), revoking access (Carr, 2023; Altulaihan et al., 2022), cybersecurity frameworks (Giuca et al., 2021; Jarjoui and Murimi, 2021), AI monitoring

(Chakraborty et al., 2023; Jimmy, 2021) and Quantum-resistant encryption (Baseri et al., 2024; Rahul et al., 2024). This study further investigates the importance of conducting thorough background checks and balancing automation and physical security, which the above researchers did not examine.

3. How does identifying cybersecurity risks associated with digital banking automation technologies in the future of work in South Africa impact the skills gap in cybersecurity professionals? The fourth question addresses how the rapid adoption of digital banking automation in the future of work in South Africa affects the skills gap among cybersecurity professionals. The growing use of digital banking automation in South Africa is expected to worsen the shortage of cybersecurity professionals in several ways. These are increased attack surface (Dillon et al., 2021; Shahraki et al., 2022), evolving threats (Umoga et al., 2024; Kayode-Ajala, 2023), demand for specialised skills (Jordan, 2022; Jurczuk and Florea, 2022) and current skills gap (Nizami et al., 2022; Jordan, 2022). Jordan (2022) examines the upskilling of existing cybersecurity professionals and encourages more students to pursue careers in cybersecurity. This research study promotes collaboration between the public and private sectors, encouraging more investment in cybersecurity education and training programs; however, none of these researchers have examined this aspect.

2.2 Definition of topic or background discussion

Automation Technologies involve using real or virtual robots, including application bots, to automate repetitive processes (Mohammad and Surya, 2018).

Cybersecurity Risk is defined as the likelihood that a sociotechnical system will be harmed or fail, depending on several known and unknown factors, including human behaviour, an individual's perception of risk, and physical and cybersecurity vulnerabilities in the system that impact control, prioritisation of resources, and system functionality (Cains et al., 2022).

Digital banking integrates technology into every aspect of financial services operations (Sanmath, 2019).

Digital Transformation in the banking industry is defined as the sector's current major transition towards digitalisation, leading to a fundamental overhaul of the banking system (Omarini, 2017). The banking industry's evolution presents new opportunities for banks to engage with customers (Omarini, 2017). Emerging technologies are poised to transform and permanently reshape the value chain of financial services (Omarini, 2017). Adapting to change and implementing new programs are crucial for the digital transformation of a bank (Khanboubi and Boulmakoul, 2019).

The future of work is a projection of the changes that work, labour, and the workplace will undergo in the following years (SHRM, 2023). It is shaped by essential factors like attracting new talent, developing strong leaders, and establishing a competitive organisation (Morgan, 2014).

2.3 Cybersecurity threats posed by automation technologies in the future of work in digital banking

Based on a literature search, this section examines cybersecurity threats resulting from increased reliance on automation technologies. It also discusses the impact of cybersecurity threats on the workforce and the skills gap. Lastly, it examines cybersecurity threats in digital banking and the regulatory challenges they pose. There is also a need to consider the new threats that automation technologies may pose to the future of work in digital banking.

2.3.1 *Cybersecurity threats resulting from reliance on automation Technologies*

Cybersecurity risks remain today due to the increased reliance on automation technologies (De Azambuja et al., 2023; Yaacoub et al., 2022). The increase in interconnectivity and reliance on digital channels exposes vulnerabilities in cybersecurity (Aithal, 2023). The way automation technologies are used has undergone significant changes (Lone et al., 2023). Organisations primarily use technology-driven strategies to address cybersecurity threats (Nobles, 2022).

The emergence of new automation technologies presents fresh risks in cybersecurity, as they can lead to potential security attacks and result in complex threats (Tao et al., 2021).

2.3.2 *Cybersecurity threats impact the workforce and the skills gap*

The frequency of cybercrime is increasing, and digital banking is constantly under attack (Monteith et al., 2021). This has led to a growing need for cybersecurity professionals with the skills to protect against these threats (Crumpler and Lewis, 2022). Unfortunately, there is a lack of qualified workers to meet this demand (Furnell, 2021). The digital banking industry is vulnerable due to a shortage of cybersecurity experts (Nobles, 2022). Digital banking with unfilled cybersecurity positions is at a higher risk of experiencing breaches, resulting in financial losses, data breaches, and damage to their reputation (Wittkop, 2022). Attackers can exploit even minor human errors resulting from a lack of cybersecurity awareness (Lee and Armstrong, 2023). Addressing the gap involves upskilling and reskilling (Ajayi and Udeh, 2024), focusing on soft skills (Bingle, 2022), expanding the talent pool (Crumpler and Lewis, 2022), and, importantly, promoting cybersecurity careers to attract more talent to the field (Furnell, 2021).

2.3.3 *Cybersecurity Risks in digital banking and its Regulatory challenges.*

The cybersecurity risks posed by the automation technologies of the future of work in digital banking are significant and diverse. These include phishing attacks (Alkhalil et al., 2021; Jain and Gupta, 2022; Basit et al., 2021), password attacks (Guan and Chen, 2022; Islam et al., 2023), insider attacks (Daubner et al., 2023) (Abulencia, 2021), social engineering attacks (Syafitri et al., 2022; Fuertes et al., 2022), malware attacks (Selvaganapathy et al., 2021; Roseline and Geetha, 2021), ransomware attacks (Reshmi, 2021; Kara and Aydos, 2022), and DDOS attacks (Lee and Armstrong, 2023; Mittal et al., 2023). These threats can cause severe financial and reputational damage, making it crucial for digital banking institutions to be cautious and prepared.

Phishing is the act of hackers sending deceptive digital communications (Lee and Armstrong, 2023). Password attacks involve hackers repeatedly trying to replicate a valid login or password sequence (Islam et al., 2023). Individuals with authorised access can inappropriately and deceitfully abuse their credentials to steal data, damage systems, and engage in other malicious activities (Daubner et al., 2023). Social engineering often involves scammers contacting users and persuading them that they are someone else (Lee and Armstrong, 2023). Malware is a software code typically introduced into systems when users open infected files (Yong Wong et al., 2021). Ransomware is a specific form of malware that warrants a separate discussion (Lee and Armstrong, 2023). Distributed denial-of-service (DDoS) attacks involve hackers submitting high-volume, high-velocity service requests to a web service from multiple sources (Lee and Armstrong, 2023).

Staying abreast of the changing digital environment presents difficulties for regulators, as they must balance security with the effective development of secure automation technologies (Nguyen and Tran, 2023). Maintaining a balance between the necessity of data collection for security reasons and safeguarding user privacy is a complex challenge (Nguyen and Tran, 2023). Effective regulation requires international cooperation due to cybercriminals' ability to operate across borders (Bechara and Schuch, 2021).

Digital banks in South Africa should invest in solid cybersecurity measures, educate employees, and enforce rigorous authentication protocols (AL-Hawamleh, 2023). Customers must exercise caution when dealing with emails and texts, utilise robust passwords and multi-factor authentication, and ensure their software is updated (Efijemue et al., 2023). Regulators should work on creating and revising regulations dealing with emerging threats, fostering international collaboration, and encouraging information sharing (McIntosh et al., 2024).

2.3.4 *Proposition 1*

New cybersecurity threats will emerge as automation technologies transform the Future of Work in digital banking.

2.4 How the South African digital banking industry mitigates the cybersecurity-attack risk identified by automation technologies.

The literature showed that the South African digital banking industry mitigates the risk of cybersecurity-attacks identified through the following: hiring skilled cybersecurity staff (Crumpler and Lewis, 2022; Jordan, 2022); staff training (Dash and Ansari, 2022; Okafor et al., 2023), digital identity (Binhammad et al., 2024; Chakraborty et al., 2023), collaboration (Polis, 2023; Jimmy, 2021), dealing with work-from-home (Dai et al., 2023; Pranggono and Arabo, 2021), cutting-edge cybersecurity software (Shwedeh et al., 2023; Lee and Armstrong, 2023), revoking access (Carr, 2023; Altulaihan et al., 2022), cybersecurity frameworks (Giuca et al., 2021; Jarjoui and Murimi, 2021), AI monitoring (Chakraborty et al., 2023; Jimmy, 2021) and Quantum-resistant encryption (Baseri et al., 2024; Rahul et al., 2024). There is a need to leverage automation technologies to improve the operational efficiencies of digital banking.

2.4.1 *Digital banking is vulnerable to cybersecurity threats due to the adoption of automation technologies.*

Automation technologies create additional opportunities for criminals to exploit, such as through mobile banking apps, online banking platforms, and interconnected systems (O'Hagan, 2023; Oyewole et al., 2024). Criminals are becoming more adept at utilising automation technologies to carry out advanced attacks (Ibrahim, 2022). Users can be deceived through social engineering tactics, leading them to disclose information or click on malicious links (Syafitri et al., 2022). Advanced AI-powered malware can circumvent traditional security measures (Maddireddy and Maddireddy, 2023). Banks may prioritise faster transactions at the expense of robust authentication processes (Ahmed et al., 2024).

MITIGATING CYBERSECURITY RISKS	DESCRIPTION
Hiring skilled cybersecurity staff	Proficient cybersecurity personnel are essential. Nonetheless, there is a significant shortage of these professionals, with many demanding high salaries due to increased specialisation and limited availability. Survey results indicate that the industry must expand by approximately 89% globally to address this gap.
Staff training	As noted, cybercrime often stems from human actions. Employees must receive regular training and ongoing reminders about the types and nature of cybersecurity threats, as well as the necessary knowledge to respond effectively.
Digital Identity	The World Economic Forum recommends a complete revamp of digital identity frameworks.
Collaboration	No organisation can stand alone. Threats are too persistent, and banks' attack surfaces are too widely spread across multiple vectors. No single bank can develop all the necessary capabilities independently. Furthermore, neutralising the source is the most effective way to combat some threats. Collaboration between banks, governments, centres of expertise, and other entities will be essential.
Dealing with work-from-home	Telecommuting expands the vulnerability of work data and systems as they are accessed through decentralised and less secure home networks. It is

	essential to develop tactics to mitigate this risk.
Cutting-edge cybersecurity software	There are many different ones available.
Revoking access	It is crucial to promptly revoke insider credentials upon termination to prevent future access to systems.
Cybersecurity Framework	To guide thorough responses and provide rich data, banks should make use of extensive cybersecurity frameworks and knowledge bases, such as NIST or MITRE ATT&CK.
AI monitoring	Creating artificial intelligence (AI) systems that track and stop hacking is a desirable path in the future. Software robots can audit simple problems, but more work needs to be done to create bots that can learn and become more adept at identifying intrusions. An additional option is an AI digital assistant that monitors staff behaviour and provides alerts about potential social engineering or other strategies to extract information from them.
Quantum resistant encryption	Research is being conducted on improved encryption that can withstand computers, although it is not yet fully perfected.

Table 2.1: Ways of mitigating cybersecurity risks in digital banks. (Lee and Armstrong, 2023, p.259).

2.4.2 *Connection between automation technologies and the emergence of new cybersecurity risks*

The expansion of connected devices and systems through automation technologies creates a larger target for hackers (Aslan et al., 2023). Identifying and fixing vulnerabilities becomes more challenging due to the complexity of automated systems (Aslan et al., 2023). Pinpointing weak spots in a complex, interconnected system can be complicated (Iacovidou et al., 2021). Relying too heavily on automation technologies can lead to a lack of human oversight and complacency (Chiou and Lee, 2023). Depending solely on automated detection may cause security teams to overlook essential signs of an attack (Alahmadi et al., 2022). Automated systems may produce false positives or miss real threats, overwhelming or giving a false sense of security to security teams (Wan and Cao, 2023). Attackers can exploit vulnerabilities in the code of automated systems (Iannone et al., 2021). Artificial intelligence (AI) or machine learning (ML) utilised in automation technologies can be vulnerable to manipulation (Bécue et al., 2021).

2.4.3 *How Automation Technologies Might Reshape the Cybersecurity Landscape in South Africa's Digital Banking.*

Digital banks can utilise tools such as Security Information and Event Management (SIEM) and User and Entity Behaviour Analytics (UEBA) through automation technologies to consistently monitor activities and detect irregularities that could indicate a cybersecurity attack (Efijemue et al., 2023). This enables quicker identification and response, reducing potential harm (Mullet et al., 2021). By automating regular tasks such as system patching and user access controls, the likelihood of human error, which is a critical factor in cybersecurity breaches, can be minimised (Yaacoub et al., 2022). Automated security operations enable Information Technology personnel to allocate more time to strategic endeavours, such as threat detection and vulnerability management (Brotherston et al., 2024).

While automation technologies are effective against known threats, cybercriminals continually devise new tactics (Sarkar et al., 2023). As a result,

security teams will still require human expertise to analyse these emerging threats and modify defences accordingly (Collins, 2022). Automated tools can generate numerous alerts, which may lead to fatigue and cause real threats to be overlooked (Ban et al., 2023). South African banks should adjust automation technologies to reduce the number of false positives (Hassan et al., 2023). Automation technology tools can be vulnerable to cybersecurity attacks, so it is essential to implement strong security measures to prevent the compromise of these tools (Aslan et al., 2023).

Despite the transformative potential of AI in enhancing cybersecurity and audit processes within digital banking, several inherent limitations pose significant challenges. One of these challenges is integrating legacy systems, as most banks operate on a patchwork of outdated systems. Integrating AI into such environments poses technical, financial, and operational difficulties (Khan and Khan, 2023). Legacy infrastructure often lacks the APIs or data pipelines necessary for real-time AI-based monitoring or auditing (Khan and Khan, 2023). Inconsistent data structures, limited interoperability, and outdated security protocols hinder the full realisation of AI's potential in enhancing cybersecurity or audit effectiveness (Khan and Khan, 2023). Data Quality and Bias Risks: AI systems are only as good as the data on which they are trained. Poor data quality, incomplete records, or historically biased datasets can lead to skewed outputs, particularly in fraud detection or risk scoring (Oguntibeju, 2024). In audit settings, this could reinforce existing systemic biases or produce misleading insights that impact decision-making (Oguntibeju, 2024).

2.4.4 *Proposition 2*

South Africa's digital banking sector can leverage automation technologies to enhance operational efficiency and proactively mitigate cybersecurity threats from its growing reliance on automated systems.

2.5 Identifying how the rapid adoption of digital banking automation technologies impacts the skills gap in cybersecurity professionals.

This section examines the rapid adoption of digital banking automation technologies, the future of work in South Africa, and the impact on the skills gap in cybersecurity professionals.

2.5.1 *Rapid adoption of digital banking automation technologies.*

Adopting digital banking automation technologies rapidly transforms the South African banking industry (Lottu et al., 2023). This pattern is supported by multiple factors, including an increase in the use of smartphones. Due to the increasing number of South Africans using smartphones, digital banking is a practical and easily accessible choice (Gertze and Petersen, 2024). Efficiency demand: Automation technologies enable banks to lower expenses, expedite customer service, and simplify procedures (Villar and Khan, 2021). Growth of Fintech Startups: These businesses are upending the established banking model by offering cutting-edge digital solutions (Arnaut and Bećirović, 2023).

Here are some examples of how digital banking automation technologies are utilised in South Africa: Robotic Process Automation (RPA) programs automate routine tasks, such as loan processing, account opening, and fraud detection (Villar and Khan, 2021; Kumar et al., 2023). Artificial Intelligence (AI): Chatbots with AI capabilities to reply to customer queries and provide customised financial guidance (Krishnan et al., 2022). Banks use big data analytics to analyse customer behaviour and develop targeted marketing campaigns and risk-reduction strategies (Cornwell et al., 2023; Chaudhary and Alam, 2022). The rapid adoption of new automation technologies has a significant impact on the banking industry in South Africa (Molopyane, 2021). Understanding the benefits and drawbacks of this trend is essential.

2.5.2 *Future of work in South Africa.*

There are several reasons why the nature of work in South Africa is likely to change significantly, and digital banking automation technologies are one of the

primary ones (Naidoo, 2021). Here is a summary of some essential elements: Automation Technologies and Job Loss. Automation technologies increase productivity, but also raise concerns about job displacement (Shetty, 2022). Banking jobs that require repetitive work, like data entry or loan processing, could become automated (Shidaganti et al., 2023). Creating New Roles with automation technologies will also lead to new job opportunities (Tschang and Almirall, 2021). Data analysis, cybersecurity, and user experience (UX) design experts will be in high demand as banks adapt to the evolving digital landscape (Oladipo et al., 2024). Changing Skill Sets: Current employees must adapt by acquiring new skills to remain competitive (Kaur et al., 2021). Upskilling and constant learning will be essential to closing the skills gap between traditional training and modern workplace demands (Ajayi and Udeh, 2024).

Other reasons include the Gig Economy and Flexible Work: As digital platforms gain traction, the gig economy may expand, providing more flexible work options for specific individuals (Montgomery and Baglioni, 2021). However, this trend also raises concerns about social protection and job security (Montgomery and Baglioni, 2021). Automating digital banking will have a wide range of future effects on South Africa's workforce (Li, 2022). Although there are obstacles, there are also opportunities to create new employment and develop a workforce with more advanced skills.

2.5.3 *Impact on the Skills Gap in Cybersecurity Professionals.*

The swift integration of digital banking automation technologies in South Africa presents a dual challenge for cybersecurity experts (Mphahlele, 2024). The impact on the current skills gap is as follows: Enhanced Attack Surfaces and Dangers - Automation technologies create new vulnerabilities. There are more points of entry for attackers to exploit as more processes become automated (Aslan et al., 2023). Cybercrime targeting automation technologies is on the rise: Cybercriminals will create strategies to attack automated systems, necessitating the need for defenders skilled in these domains (Jarrett and Choo, 2021). Increased surface area of attack: As the use of Internet of Things-connected devices and systems grows, attackers have a larger canvas to work with (Sviatun et al., 2021).

Shifting Proficiency Needs: Specialised skills are required for cybersecurity professionals (Furnell, 2021). These include knowledge of protecting automated systems, utilising data analytics to identify anomalies, and responding promptly to incidents involving rapidly evolving threats (Naseer et al., 2021). Information Technology and security convergence: There is a growing blurring of the boundaries between Information Technology operations and security (Shepherd, 2021). Experts with in-depth knowledge of both fields will be in great demand (Trim and Lee, 2021). The significance of soft skills: To effectively collaborate, communicate, and think critically with other teams and stakeholders, cybersecurity professionals must possess these abilities (Pirta-Dreimane et al., 2023).

Reducing the Skills Gap: Academic and training establishments must modify their curricula to provide students with the most recent knowledge of cybersecurity and automation technologies (AlDaajeh et al., 2022). Initiatives for reskilling and upskilling: Ongoing training programs are necessary for seasoned cybersecurity professionals to stay current with the constantly changing threat landscape (Toth and Erdődi, 2023). Encouraging women and minorities to pursue careers in cybersecurity can help address the talent shortage (DeCrosta, 2021). This is one way to promote diversity in the cybersecurity industry. South Africa can guarantee a robust cybersecurity workforce prepared to protect the development of digital banking by taking proactive measures to close the skills gap (Jordan, 2022).

Cybersecurity risks are not purely technical, but are deeply intertwined with human behaviour, decision-making, resistance to change, and skills deficits within organisations. For example, insider threats, social engineering, and poor cybersecurity awareness among employees are critical vulnerabilities. Moreover, the cybersecurity skills gap is an essential human factor that is thoroughly examined in the study. This section discusses how the rapid adoption of automation technologies in South Africa’s digital banking sector has intensified the demand for cybersecurity professionals with both technical and soft skills, including critical thinking, communication, and adaptability. These skill deficits directly contribute to cybersecurity exposure and risk.

2.5.4 *Proposition 3*

The rapid growth of digital banking automation technologies will impact the cybersecurity skills gap in South Africa’s future workforce.

2.6 Analytical Framework

The analytical framework is an integrated overview of this study's theoretical and empirical concepts.

2.6.1 *Theoretical Framework*

The theoretical framework of this study is derived from the following theories. The NIST Risk Management Framework (RMF) is a comprehensive, flexible, and repeatable process designed to manage and reduce cybersecurity and privacy risks for organisations and systems (Efe, 2023). Developed by the National Institute of Standards and Technology (NIST), the RMF provides a structured approach to integrate security, privacy, and supply chain risk management activities into the system development lifecycle (Force, 2017).

The RMF consists of seven core steps:

- Categorize Information Systems: Determine the impact of a potential loss of confidentiality, integrity, or availability of information.

- Select Security and Privacy Controls: Select appropriate security controls based on the system's categorisation and risk assessment.

- Implement Security and Privacy Controls: Put the selected controls in place.

- Assess Security and Privacy Controls: Evaluate the effectiveness of the implemented controls.

- Authorize Information System: Make a formal decision to operate the system based on the assessment results.

- Monitor Security and Privacy Controls: Continuously monitor the system's security and privacy posture.

- Review Security and Privacy Controls: Periodically review the RMF process and make necessary adjustments (Efe, 2023).

The RMF's benefits include its comprehensiveness, addressing security, privacy, and supply chain risks. It is also flexible and can be adapted to organisations of all sizes and industries. It is repeatable by providing a structured process for ongoing risk management. It is measurable and allows for the evaluation of risk management effectiveness. It is Cost-effective, which helps prioritise resources and focus on the most critical risks (AlSadhan, 2022).

We considered the Diffusion of Innovation Theory to provide a theoretical foundation for the research problem (Greenhalgh et al., 2008). This theory explores how innovations are adopted and spread within a population (Wani and Ali, 2015). It can be used to analyse the factors influencing the adoption of automation technologies in the South African digital banking industry. The NIST RMF can be integrated with the theoretical framework to provide a more comprehensive understanding of the cybersecurity risks associated with automation technologies in digital banking. Risk Identification and Assessment involve the Diffusion of Innovation Theory, which Identifies factors that may influence the adoption of risky automation technologies (Rodríguez-Espíndola et al., 2022). Diffusion of Innovation Theory Identify factors that may influence the adoption of risk mitigation measures (Wejnert, 2002).

Risk Monitoring and Review: Diffusion of Innovation Theory monitors the adoption and spread of automation technologies and risk mitigation measures (Molinillo and Japutra, 2017). By integrating the NIST RMF with the theoretical framework, the research can provide a more nuanced understanding of the cybersecurity risks associated with automation technologies in digital banking. This includes identifying specific risks associated with different types of automation technologies, understanding the factors that influence stakeholders' perceptions of these risks, developing effective risk mitigation strategies that address both technical and social aspects, and evaluating the impact of risk

mitigation measures on adopting automation technologies and the overall security of digital banking systems.

Also, ISO 27005 a framework for Information Security Risk Management (Al-Mudaires et al., 2023) was used. It is an international standard that provides guidelines for managing information security risks (Al-Mudaires et al., 2023). It is a crucial component of the broader ISO 27000 family of standards, forming an Information Security Management System (ISMS) (Fonseca-Herrera et al., 2021). The critical focus of ISO 27005 is that the standard offers a structured approach to identifying potential threats and vulnerabilities, assessing the impact of those threats, evaluating the overall risk and treating the identified risks (Kitsios et al., 2022).

How ISO 27005 Works is as follows: Risk Identification involves identifying potential threats, vulnerabilities, and assets. Risk Analysis consists of assessing the likelihood and potential impact of threats materialising. Risk Evaluation involves determining the overall significance of the identified risks. Risk Treatment deals with deciding on appropriate actions to manage the risks, such as accepting, transferring, mitigating, or avoiding them. Risk Monitoring and Review involve continuously evaluating the effectiveness of risk management measures (Alheadary, 2023).

The benefits of Implementing ISO 27005 are improved risk management, which provides a systematic approach to identifying and managing risks; compliance, which supports compliance with other standards and regulations; enhanced decision-making, which offers data-driven insights for risk-based decisions; and reduced losses, which help protect assets and minimise the impact of incidents. Increased stakeholder confidence demonstrates a commitment to information security (Al-Ahmad and Mohammad, 2013).

Total Quality Management (TQM) is a philosophy that emphasises continuous improvement and customer satisfaction (Bahia et al., 2023). By integrating ISO 27005 into TQM practices, digital banks can enhance their cybersecurity posture and achieve higher levels of quality (Kitsios et al., 2023). ISO 27005 can be applied to TQM in the context of the research problem through Risk-

Based Quality Management: TQM can be adapted to incorporate a risk-based approach, prioritising quality initiatives based on their potential impact on cybersecurity (Björnsdottir et al., 2022). Continuous Improvement: ISO 27005's framework can be used to identify and address cybersecurity risks as they evolve, ensuring that quality initiatives remain aligned with the organisation's changing security needs (Calder, 2023).

Customer Satisfaction: By mitigating cybersecurity risks, organisations can significantly enhance customer confidence and satisfaction, which is a crucial goal of TQM (Kemendi and Michelberger, 2024). Supplier Management: TQM's focus on supplier relationships can be extended to include cybersecurity assessments, ensuring that suppliers meet the organisation's security standards (Kemendi and Michelberger, 2024). Employee Training: TQM's emphasis on employee training can be leveraged to provide employees with the necessary skills to identify and mitigate cybersecurity risks (Arora and Gupta, 2020). By applying ISO 27005 to TQM, digital banks can identify and assess the cybersecurity risks associated with automation technologies. They can also develop and implement effective risk mitigation strategies to address these risks. They can monitor and review the effectiveness of risk management measures. They can also ensure that quality initiatives are aligned with the digital banks' cybersecurity objectives. Enhance customer confidence and satisfaction by demonstrating a commitment to cybersecurity.

Other theories include management theories, which encompass the following: Organisational Behaviour Theories – Resistance to Change. Organisational Behaviour (OB) theories suggest that employee attitudes, motivation, and culture influence the success of technology adoption and security protocols (Delso-Vicente et al., 2025). Leadership Theories – Transformational Leadership: Transformational leadership theory emphasises leaders who inspire, motivate, and empower employees to embrace change and innovate (Magasi, 2021). IT Governance Frameworks – COBIT & ISO/IEC 38500: The management of IT risks and compliance can be better structured using governance frameworks such as COBIT (Control Objectives for Information and Related Technologies) and ISO/IEC 38500, which define decision-making rights

and responsibilities (Momani, 2024). Change Management Theory – Kotter's 8-Step Model: John Kotter's change management model outlines eight sequential steps to lead successful organisational transformation, including creating urgency, forming guiding coalitions, and embedding new approaches (Carreño, 2024).

2.6.2 *Conceptual Framework*

This conceptual framework examines the cybersecurity risks related to automation technologies in the context of the future of work in the digital banking industry in South Africa. It integrates insights from the NIST Risk Management Framework (RMF) and ISO 27005.

Automation Technologies (AT): These encompass automation technologies used to automate banking sector tasks, such as Artificial Intelligence (AI), Machine Learning (ML), and Robotic Process Automation (RPA) (Mahalakshmi et al.,2022). Incorporating digital technologies into every aspect of a bank's operations and customer interactions is known as digital transformation (DT) (Kraus et al., 2021).

Future of Work (FoW): How work is changing in the digital banking industry, including how skill sets change, how humans and machines collaborate, and how jobs may be eliminated (Parker and Grote, 2022). Cybersecurity Risks (CR) are threats and vulnerabilities resulting from using automation technologies in digital banking and could cause financial losses, reputational harm, and data breaches (Nicoletti and Nicoletti, 2021). The study of the NIST Risk Management Framework (RMF) and ISO 27005 examines and looks at the core principles of Risk Management, process-oriented approach, compliance and regulatory alignment, organisational alignment and effectiveness and efficiency (Σαμπάνης, 2024).

The relationship between cybersecurity risks (CR) and Automation Technologies (AT) is that due to automation technologies' increased reliance on intricately linked systems, cybercriminals now have access to new attack vectors and vulnerabilities (Mallick and Nath, 2024). The relationship between Cybersecurity Risks (CR) and Digital Transformation (DT) is that as banks put

speed and efficiency ahead of thorough security implementation, the quick speed of digital transformation could result in security lapses (Murinde et al., 2022). The relationship between Cybersecurity Risks (CR) and the Future of Work (FoW) is that hackers may be able to take advantage of weaknesses in the workforce due to changes like a skills gap or less human oversight (Jordan, 2022).

The relationship between the NIST Risk Management Framework and Cybersecurity Risks (CR) is that the NIST Risk Management Framework (RMF) is a structured approach to managing cybersecurity risks (Yulianto and Soewito, 2023). It provides a systematic process for identifying, assessing, and mitigating the threats that could compromise an organisation's systems and data (Holmes, 2021). The relationship between ISO 27005 and Cybersecurity Risks (CR) is that ISO 27005 is essentially the blueprint for managing cybersecurity risks (Taherdoost, 2022). It provides a structured approach to identifying, assessing, treating, and monitoring information security risks, including cybersecurity-related ones (Shikhaliyev, 2024). The conceptual framework diagram is shown in Figure 1 in section 1.1.

2.7 Conclusion of Literature Review

This study investigates the intricate connection between cybersecurity and automation technologies in South Africa’s future digital banking environment. The study looks at the effects of growing automation technologies on the workforce's skill set, changing regulations, and cybersecurity threats. After that, it examines how digital banks can reduce these risks and considers how automation technologies might change cybersecurity. Lastly, the study investigates how South Africa's cybersecurity skills gap is affected by the country's quick adoption of automation technologies. Understanding these issues prepares the digital banking industry for an automated and secure future. Three Propositions were drawn. Propositions 1, 2 and 3 are stated in subsections 2.3.4, 2.4.4 and 2.5.4, respectively.

CHAPTER 3. RESEARCH METHODOLOGY

This chapter meticulously outlines the comprehensive research methodology, encompassing the research paradigm, research approach, research design, data collection methods, population and sample, research instruments, data collection procedures, data analysis strategies, and interpretation. It also addresses the potential limitations and challenges of the study, as well as quality assurance and ethical considerations, ensuring a thorough and robust research process.

3.1 Research Paradigm

This study employed the interpretivist paradigm, which enabled the use of qualitative research methods (Hennink et al., 2020). It emphasises understanding the subjective meanings people attach to their experiences (Fossey et al., 2002) and employs techniques such as interviews, observations, and document analysis (Cuthbertson et al., 2020).

Interpretivism is a research philosophy that emphasises the subjective nature of human experience and the importance of understanding social phenomena from the perspective of those involved (Acharya, 2024). It assumes that reality is socially constructed and that meaning is created through social interaction (Pervin and Mokhtar, 2022). Researchers using this approach seek to interpret and understand the world through the eyes of their participants (Knotter, 2022). The research aim is to "identify cybersecurity risks in automation technologies in the future of work in the digital banking industry in South Africa". An interpretive approach focused on understanding how individuals within the digital banking industry perceive and experience cybersecurity risks related to automation technologies. Instead of simply identifying risks, the research delved into the meanings and interpretations these individuals attach to these risks. Interpretivism suggests that respondents actively construct social reality (Irshaidat, 2022). The respondents in this study are employees in the digital banking industry who are directly or indirectly involved with automation

technologies. Their experiences, perspectives, and interpretations of cybersecurity risks were central to the study.

Given the nature of this study, respondents shared various experiences related to cybersecurity in digital banking. Some potential experiences include:

- Direct exposure to cybersecurity incidents involved personal experiences with data breaches, phishing attacks, or other cybersecurity threats (Pugnetti et al., 2021).
- Concerns about job security: Automation technologies might lead to fears of job displacement, which could influence perceptions of cybersecurity risks (Borgia et al., 2022).
- Challenges adapting to new technologies: Respondents struggled to understand and implement cybersecurity measures in an increasingly automated environment (Thishopana and Arulrajah, 2023).
- Lack of awareness of cybersecurity risks: Some individuals had limited knowledge of the potential threats of automation technologies (Kuraku et al., 2023).
- Trust issues: Respondents expressed concerns about the reliability and security of automated systems (Melnyk, 2024).
- Ethical considerations: Some individuals raised ethical concerns about the use of automation technologies in banking, particularly regarding privacy and surveillance (Prastyanti et al., 2023).

By examining these experiences through an interpretive lens, one gains a deeper understanding of the complex interplay between human factors, technology, and cybersecurity in the digital banking industry.

3.2 Research approach

This study adopted qualitative research methods. Qualitative research is an exploratory approach that delves into participants' subjective experiences to understand their perspectives and meanings (Lim, 2024). Researchers employ interviews, observations, and document analysis to gather rich, non-numerical data, uncovering patterns, themes, and insights (Lim, 2024). This inductive

process enables the development of theories grounded in real-world experiences, providing a deeper understanding of complex social and human phenomena (Mitchell and Cody, 1993).

3.3 Research design

The research design used in this study is Phenomenology. Phenomenology focuses on understanding the lived experiences of individuals (Van Manen, 2017). Researchers aim to describe and interpret the essence of a phenomenon as experienced by participants (Dangal and Joshi, 2020). It involves in-depth interviews and reflective analysis to uncover the shared meanings and structures of experiences (Alhazmi and Kaufmann, 2022).

3.4 Data collection methods

The data collection methods used for this study were semi-structured interviews. Interviews are an excellent means of obtaining comprehensive details and comprehending the “why” behind things (Rosenthal, 2016). We can elicit more information and ask follow-up questions during an interview (Roberts, 2020). This was helpful because this study comprehended people's experiences or opinions to answer the research questions.

3.5 Population and sample

This study gathered data from the management staff of the information technology departments of digital banks in South Africa. A sample of ten managerial staff members of the information technology department of digital banks was drawn through interviews. Samples were drawn from five digital banks in Gauteng Province. These banks are Absa Bank, Standard Bank, Discovery Bank, Nedbank, and FNB. Two participants were selected from each of these banks, from which samples were collected.

3.5.1 *Population*

Population is the total collection of elements we wish to make inferences (King et al., 2021). A population of ten information technology managerial staff in digital banks was interviewed. It was challenging to reach respondents (Nel and Boshoff, 2021).

3.5.2 *Sample and sampling method*

The sample was chosen for this study due to its lower cost, as it offers an incredible speed of data collection, facilitates a faster understanding of the population and its characteristics, and allows for inference to be drawn (Lakens, 2022). The sample tells how to reduce the total population to a manageable size (Blake, 2022). The purposive sampling method was applied. Purposive sampling is a non-probability technique where researchers strategically select participants based on specific characteristics relevant to their study (Adebayo and Ackers, 2021). The goal was not to achieve a statistically representative sample of the whole population. Instead, the researcher selected individuals who provided rich insights into the topic, enabling an in-depth exploration of specific experiences or perspectives (Renjith et al., 2021). This method benefits qualitative research and studies focusing on a particular subgroup within a larger population (Pace, 2021).

A sample was required due to the structure of the research questions, which necessitated that respondents participate based on their opinions and experiences. The respondents were convinced that participating would enable them to cross-check whether they were current with the latest information from the research body of knowledge through the questions asked during the interviews. A sample of 10 respondents was used, and the sample also reached a saturation point, where no new themes emerged from the research (Naeem et al., 2024). The ten participants were from five out of the seven digital banks in South Africa. There are seven digital banks in South Africa (Shumba, 2023).

The participants' selection criteria were based on their role as managers in digital banking. The participants' experience levels ranged from 14 to 24 years.

They were between the ages of 40 and 55 years. Their Nationality was mainly South African, with others being Nigerians and from the UAE. The participants' races were black/African and coloured.

3.6 The research instrument

The research instruments used in this study are interview schedules (see the appendix). The interview was also used because the study needs detailed information and wants to explore the topic in depth (Osborne and Grant-Smith, 2021).

3.7 Procedure for data collection

A letter was sent to the information technology managers of digital banks in South Africa, stating that each bank had been identified as one of the few digital banking spaces in South Africa known for its innovation and customer security. This study required data from these managers. A face-to-face or Team interview was conducted with the information technology managers of the selected banks. The meeting was recorded using a voice recorder with their permission, estimated to last an average of 45 minutes.

3.8 Data analysis strategies and interpretation

The data analysis strategy and interpretation in this study employed thematic analysis. Thematic analysis is primarily qualitative (Christou, 2022). It involves identifying, analysing and interpreting patterns of meaning (themes) within qualitative data (Vaismoradi et al., 2016). The themes were analysed through quotations, phrases, and charts. Categories and codes were also generated and analysed (see appendix). Additionally, the analysis was conducted manually and using ATLAS.ti 25. ATLAS.ti is a powerful software tool to help researchers analyse qualitative data (Gupta, 2024). It is a sophisticated digital workbench for non-numerical information, such as text documents, audio and video files, and images (Gupta, 2024). ATLAS.ti helps researchers make sense

of this data in organisation, coding and analysis, visualisation, collaboration and reporting (Gupta, 2024).

ATLAS.ti is widely used in various fields, including the social sciences. Researchers in sociology, psychology, education, and other social science disciplines use ATLAS.ti to analyse qualitative data from interviews, focus groups, and observations (Smit, 2021). In essence, ATLAS.ti helps researchers to manage large amounts of qualitative data efficiently, identify and analyse key themes and patterns in their data, visualise the connections between different aspects of their research, collaborate with other researchers on joint projects, and generate comprehensive reports of their findings (Smit, 2021). Table 3.2 below shows the consistency table.

Table 3.2. Consistency table: research questions, propositions, data collection and data analysis

RQ #		State Research Question or Objective	Prop/hyp #	State Proposition or Hypothesis	Data collection detail	Data analysis method
1		What are the cybersecurity threats posed by automation technologies of the future of work in digital banking?	1	New cybersecurity threats will emerge as automation technologies transform the Future of Work in digital banking.	Interview guide questions 1, 2 and 3.	Thematic analysis.
2		How can the South African digital banking industry mitigate the cybersecurity risks identified from bringing on board automation technologies for the future of work in the banking sector?	2	South Africa's digital banking sector can leverage automation technologies to enhance operational efficiency and proactively mitigate cybersecurity threats from its growing reliance on automated systems.	Interview guide questions 4 and 5.	Thematic analysis

RQ #		State Research Question or Objective	Prop/hyp #	State Proposition or Hypothesis	Data collection detail	Data analysis method
3		How does identifying cybersecurity risks associated with digital banking automation technologies in the future of work in South Africa impact the skills gap in cybersecurity professionals?	3	The fast-growing use of digital banking automation technologies will affect the cybersecurity skills gap in South Africa's future workforce.	Interview guide questions 6, 7 and 8.	Thematic analysis

3.9 Possible limitations and challenges of the study

Limitations:

- Evolving nature of cybersecurity threats: The rapid pace of technological advancements and the emergence of new cybersecurity threats limited the generalizability of findings to future scenarios.
- Access to participants: Due to time constraints and confidentiality concerns, securing interviews with key stakeholders in the digital banking industry proved challenging, especially those with in-depth knowledge of automation technologies and cybersecurity.
- Depth of information: While qualitative research provides rich insights, it does not offer a comprehensive overview of cybersecurity risks across the entire banking industry in South Africa, as it focuses primarily on digital banking.
- One limitation of the study is that the findings are context-specific and not generalizable to the entire sector without further quantitative analysis.

Challenges:

- Defining "future of work": The "future of work" concept is ambiguous and subject to interpretation. Clearly defining the scope of this study was essential.
- Uncovering latent risks: Identifying emerging cybersecurity risks associated with automation technologies required a deep understanding of both domains, which was challenging for researchers without technical expertise.
- Participant bias: Participants hesitated to disclose sensitive information about cybersecurity vulnerabilities due to concerns about reputational damage or legal implications.

- Data analysis: Analysing qualitative data, mainly when dealing with complex and technical topics, was time-consuming and required strong analytical skills.

3.10 Quality Assurance

This section examines the concepts of transferability, dependability, credibility, and confirmability that apply to the qualitative research used in this study. These concepts check the quality assurance of this study's qualitative research.

3.10.1 *Transferability*

Given the unique context of South Africa's digital banking industry, transferability was a challenge (Umar, 2022). This study meticulously documented the research context to maximise transferability, including the specific characteristics of the South African banking landscape and regulatory environment (Lekhelebana, 2022). This study employed theoretical frameworks that have broader applicability and explored potential similarities with other contexts (Constantino et al., 2021). By providing rich, detailed descriptions of the research process and findings, this study would enable readers to assess the transferability of the results to their settings (Stalmeijer et al.,2024).

3.10.2 *Dependability*

Dependability was challenging due to the evolving nature of automation technologies and the dynamic digital banking landscape (Abdulhamid et al., 2022). This study employed rigorous methodological triangulation involving multiple data collection and analysis techniques to enhance dependability (Amin et al., 2020). Additionally, this study conducted member checking and peer review to ensure the credibility and trustworthiness of the findings (Motulsky, 2021). By providing detailed documentation of the research process, including data collection instruments, analysis procedures, and decision trials, this study would enable others to assess the consistency and replicability of the study (Rogge et al., 2024).

3.10.3 *Credibility*

Enhancing credibility was crucial. Given the complex and evolving nature of cybersecurity risks in automation technologies, credibility was established through rigorous methodology, including triangulation of data sources, member checks, and peer review (Motulsky, 2021). This study provides a detailed description of the research method, data collection processes, and analytical techniques to maximise credibility, allowing for scrutiny and potential replication (Aguinis, 2023). Additionally, transparently addressing limitations and biases contribute to the study's trustworthiness (O'Kane et al., 2021).

3.10.4 *Confirmability*

Enhancing confirmability was crucial. To achieve this, this study meticulously documented the research process, including the data collection method, analysis techniques, and decision-making processes (Ahmed, 2024). This audit trail allowed for external examination and verification of the findings (Ahmed, 2024). Additionally, this study employed reflexivity to acknowledge potential biases and their influence on the research (Ahmed, 2024). By maintaining a clear separation between data and researcher interpretations, this study aims to enhance the objectivity and confirmability of the findings (Enworo, 2023).

3.10.5 Reflexivity

Reflexivity in quality assurance involves a critical self-examination of the processes, assumptions, and biases inherent in the assessment and improvement of quality (Caffer et al., 2024). It moves beyond merely checking for compliance with standards, fostering a deeper understanding of the context and the potential for unintended consequences of QA interventions (Edwards, 2023). By acknowledging that quality is not an objective, fixed target, but rather a socially constructed concept, reflexivity promotes continuous learning and adaptation within QA systems (Jansawang et al., 2025). This iterative process of reflection and action can lead to more nuanced and effective quality improvement strategies, as it allows for the questioning of established norms and the exploration of alternative approaches (Lim, 2025). Ultimately,

embracing reflexivity enhances the credibility and utility of quality assurance efforts by making them more transparent, adaptable, and responsive to the evolving needs of stakeholders (Jansawang et al., 2025).

3.11 Ethical considerations

This study ensures that this research is ethical in many ways. Each digital bank was informed about this research and our interest in collecting data from their organisations. Data from digital banks was collected through interviews. Additionally, ethics clearance letters were solicited from each bank. Additionally, the University of the Witwatersrand was requested to issue an ethics clearance certificate. Ensuring that the research was ethical involved ensuring that the individual responses from the interviewees were not identifiable nor disclosed to other participants during the data collection process.

Furthermore, this study ensured that each participant was informed of our intentions through the participant information sheet. They were all informed that their responses would not be identifiable in the final report. The final report did not disclose restricted information or analysis. The identities of respondents/participants were not needed in the raw data and final report. Bank credentials were not disclosed in the final report. Anonymity was preserved throughout. We also emphasised that participants could withdraw from the study whenever they felt threatened. All collected data was maintained in a way that respected the nature of the original participants' consent.

CHAPTER 4. PRESENTATION OF FINDINGS

4.1 Introduction

This chapter provides an overview of the study, summarising the theoretical framework, the problem, the significance, the research questions, propositions, data gathering, the data collection method, and the data analysis strategy. The chapter also includes the findings of propositions 1, 2 and 3. The findings of each proposition include the data analysis and presentation of the findings. Lastly, we close the chapter with a summary.

4.2 Overview of the study

The benefits of the ISO 27005 framework include improved risk management and compliance, enhanced decision-making, reduced losses, and increased confidence among stakeholders (Al-Ahmad and Mohammad, 2013). The benefits of the NIST Risk Management Framework include comprehensiveness, flexibility, repeatability, measurability and cost-effectiveness (AlSadhan, 2022). This study aims to identify and assess the cybersecurity risks associated with implementing automation technologies within South Africa's digital banking sector. By understanding these risks, the study seeks to develop effective mitigation strategies to protect the industry from financial loss, reputational damage, operational disruptions, legal liabilities, and national security threats. Additionally, this research explored the implications of these cybersecurity risks on the existing cybersecurity skills gap in South Africa. Essentially, the study seeks to contribute to a safer and more resilient digital banking environment in the country by providing actionable insights into cybersecurity challenges and potential solutions.

This research explores three research questions, as outlined in Section 1.4.

This study has three propositions: Proposition 1 (subsection 2.3.4), Proposition 2 (subsection 2.4.4), and Proposition 3 (subsection 2.5.4).

4.3 Findings of Proposition 1

This section presents the data analysis of Proposition 1, including the findings and conclusions of the proposition.

4.3.1 *Data Analysis of Proposition 1*

The data analysis for Proposition 1 was done manually and through Atlas ti 25. The Theme concerning the first research question was derived from its content. The first Theme is Cybersecurity Risks, which is derived from the content of the first research question.

Below is Table 4.3, titled "Interview Questions for Theme 1."

Interview Questions as per Theme 1.

Question no.	Category	Number of questions
Q1	Area	1
Q2	Vulnerability	1
Q3	Exploit	1

Table 4.3: Interview Questions of Theme 1.

Table 4.3 lists each interview question number in Theme 1, along with its corresponding category and the number of interview questions in each category. For Interview Question 1, the category is Area; for Interview Question 2, it is Vulnerability; for Interview Question 3, it is Exploit.

Below is Table 4.4. It displays the interview schedule according to Theme 1.

Interview Schedule as per Theme 1

Question no.	Question	Category
Q1	With the rapid adoption of automation technologies like AI and robotics in South African banks, the urgency of understanding	Area

	how these advancements could potentially increase vulnerability to cybersecurity attacks cannot be overstated. Are there specific areas within automated workflows that might be more susceptible to compromise?	
Q2	South African banks are automating many processes, which can introduce new cybersecurity risks. Based on your experience, what specific vulnerabilities do you see emerging from automation technologies in the digital banking industry?	Vulnerability
Q3	How can attackers exploit these vulnerabilities?	Exploit

Table 4.4: Interview Schedule as per Theme 1.

Table 4.4 lists the specific interview question number, states the corresponding interview question, and categorises each question by number.

We also present tables and figures in the Appendix concerning Theme 1. Tables 1A and 2A are in Appendix A. Theme-Category Codebook of Theme 1 is the Table in Appendix A, Table 1A. It presents the first research question, along with its theme, and the three categories: Area, Exploit, and Vulnerability, accompanied by an example of a quotation from each category. The table in Appendix A, Table 2A, shows the Category-Code codebook of Theme 1. This displays Theme 1, categories, and codes, along with a description of each code.

Figures 1A, 2A, and 3A are included in Appendix B. Figure 1A in Appendix B presents a bar chart of theme 1, which has three categories. Each category shows the number of quotations (Gr) and categories and codes (Gs). This is demonstrated across ten participants. Figure 2A in Appendix B below shows the

word frequencies for theme 1. Figure 3A in Appendix B illustrates the network of Theme 1, including its categories and codes.

4.3.2 *Proposition 1*

The findings from Research Question 1 reveal that automation technologies in digital banking introduce significant cybersecurity threats, including AI-driven attacks, API security risks, RPA vulnerabilities, and insider threats. Automated workflows, particularly those that integrate AI and third-party vendors, are vulnerable to data breaches, phishing attacks, and adversarial manipulations. Attackers exploit weak access controls, cloud security gaps, and poorly configured APIs to infiltrate banking systems. The implication is that digital banks must adopt robust security frameworks, enhance staff training, and implement AI-driven threat detection to mitigate evolving risks and safeguard financial data, maintaining customer trust and regulatory compliance in an increasingly automated landscape.

The theme of the first research question is cybersecurity threats. This section involves the theme's three categories: Area, Vulnerability, and Exploit. It includes quotations from each of the ten participants.

The table below, Table 4.5, is titled "Theme 1" and shows categories along with the number of quotations.

Theme- Cybersecurity Risks	Total number of quotations
Area (Category)	28
Vulnerability (Category)	29
Exploit (Category)	30

Table 4.5: Theme 1 presents categories along with the corresponding number of quotations.

Table 4.5 shows the three categories in the first Theme: Area, Vulnerability, and Exploits. It also shows the total quotations for each category made through

Atlas ti 25. The 10 participants' most essential quotations, which comprise almost all the quotations in each category, are stated below.

4.3.2.1 Area

Areas within automated workflows that are more susceptible to cybersecurity risks refer to specific components, processes, or integrations within a computerised system vulnerable to threats, attacks, or exploitation (Sarker, 2024). The findings from the first research question are as follows: We have the first interview question, and the category for this question is Area. There are areas within automated workflows that might be more susceptible to compromise. The category Area is derived from the theme of the first research question and the theoretical framework. This is further broken down into 10 from Participant 1 to Participant 10 and is discussed below:

4.3.2.1.1 Participant 1

Participant 1 (Male, 45) answers to the first interview question are as follows: He said:

> *"I would say Integration with third parties/vendors/partners. While SA banks pride themselves on their security, most data breaches occur in third-party/vendor/partner environments."*

He further said:

> *"Also, I would say staff training (or lack thereof). Regardless of how strong your cybersecurity is, if your staff continuously opens and clicks on foreign links, the company will be vulnerable to a breach. Banks, however, are starting to have regular training and advise employees about cyberattacks."*

4.3.2.1.2 Participant 2

What Participant 2 (44:Manager) said concerning the category Area is as follows: She said:

> *"Yes, I believe there are automated workflows that often rely on accessing sensitive customer data for decision-making, transaction processing, and service personalisation. In my experience, AI systems that manage and analyse this data can be susceptible to breaches or unauthorised access."*

She also said:

> *"In my experience, Banks have RPA and Bots, which automate repetitive tasks like back-end processing. These bots are given high access to banking systems, making them attractive targets."*

4.3.2.1.3 Participant 3

Participant 3 (Female, 42) spoke about her experience concerning specific areas within automated workflows that might be more susceptible to compromise. She said the following:

> *"In my experience, complete automation technologies with minimal human interaction could be a big issue, as machines may overlook some threats, and another process or attack can manipulate the systems. System administrators must continuously monitor entry points like API connections to detect adversaries and ensure data integrity."*

4.3.2.1.4 Participant 4

Participant 4 (Male, 48) told me about his experience concerning the category Area. He said:

> *"In my experience, robotic and Automated Processes are most vulnerable when a workflow is started and completed without human intervention. This includes credit loan applications or limit increases that do not need human process intervention."*

4.3.2.1.5 Participant 5

Participant 5 (46: Black/African), in talking about his experience, said:

> *"I believe automation technologies (AI, robotics) introduce new cybersecurity risks to South African banks. Key vulnerable areas include data integration and "APIs, AI/ML models, robotic process automation (RPA), the implementation of robust security controls, the development of incident response plans, and the investment in employee training."*

4.3.2.1.6 Participant 6

Participant 6 (a 50-year-old female) spoke about her experience with the category of Area. She said:

> *"I would say yes. Specific areas include Endpoint Devices and IoT Integration, APIs, Insider Threats, and RPA. Endpoint Devices and IoT*

Integration: These are potential entry points for attackers, particularly devices such as ATMs or mobile payment systems. APIs (Application Programming Interfaces): Vulnerabilities in APIs can lead to unauthorised access or data breaches. Additionally, there are insider threats: Automation Technologies reduces manual oversight, making it easier for insiders to exploit systems without detection. RPA (Robotic Process Automation): Bots handling sensitive data can be compromised to manipulate or extract information."

4.3.2.1.7 Participant 7

Participant 7 (45: South African) spoke extensively on specific areas within automated workflows that might be more susceptible to compromise. He said the following:

"From my experience, I have experience in third-party integrations, data entry and processing, compliance and regulatory reporting, and cloud services. Third-Party Integrations: Banks often utilise third-party services and vendors for automating various processes. These integrations can introduce security risks if the third-party systems are not adequately secured. Data Entry and Processing: Automated systems often handle large volumes of sensitive data, making them attractive targets for cybercriminals. Any vulnerability in these systems can lead to data breaches or unauthorised access."

He further said:

"In my experience, compliance and Regulatory Reporting are also important. Automated compliance checks and reporting systems must be secure to prevent tampering or manipulation, which could lead to regulatory breaches and penalties."

4.3.2.1.8 Participant 8

Participant 8 (Coloured, 51) spoke about the category area. He said:

"I think the rapid use of AI and robotics in South African banks brings excellent efficiency but also opens up some weak spots regarding cybersecurity. For example, areas such as customer authentication, particularly when using biometrics or AI-driven decisions, could be targeted due to the sensitive data involved. In my experience, Automated systems that flag suspicious transactions might also be at risk if hackers find ways to mess with the algorithms or feed them insufficient data."

He also said:

"Another concern is robotic process automation (RPA); if these bots get hacked, they could access critical systems or data. Banks need strong security, constant monitoring, and regular testing to keep these systems safe to avoid potential threats."

4.3.2.1.9 Participant 9

Participant 9 (Nigerian, 50) said:

"In my experience, South African banks are generally cautious when adopting new technologies, especially those with minimal human intervention. Among the most vulnerable aspects are the integration points between automation technology tools and legacy systems."

He also said:

"Despite extensive quality assurance processes, it often takes time to complete integrations fully. Authentication weaknesses in automation technologies are frequently overlooked during these integration phases, creating potential entry points for attackers to gain unauthorised access to systems."

4.3.2.1.10 Participant 10

Participant 10 (a 54-year-old South African) spoke broadly about the category area. He said the following:

"I would say yes. Automated banking workflows integrating AI and robotics introduce unique vulnerabilities that cybercriminals could exploit".

He further said:

"Specific areas within these workflows that are particularly susceptible include, I would say, data handling and storage. This includes Sensitive Data in Transit and Data Lakes and Storage Systems. Sensitive Data in Transit: Automated workflows frequently involve exchanging sensitive customer or transaction data across multiple systems. Improper encryption or insecure APIs could lead to data breaches. "Data Lakes and Storage Systems: AI and robotic processes generate and access large datasets. If these storage systems lack robust security measures, they can become a target for attackers."

He spoke further by saying:

"I would secondly say AI and Machine Learning Models. This includes Model Manipulation and Adversarial Attacks. Model Manipulation: AI systems rely on training data to make decisions. If the training data is

compromised (data poisoning), the AI could make erroneous decisions that could be exploited". Adversarial Attacks: attackers can craft inputs designed to confuse AI models, such as image or text alterations, causing the system to behave unexpectedly."

He also said:

"Thirdly, I would say Robotic Process Automation (RPA) Scripts. This includes hardcoded credentials and workflow exploitation. Hardcoded Credentials: RPA bots often need access to multiple systems. If credentials are hardcoded into scripts without encryption, attackers could extract them to gain unauthorised access. Workflow Exploitation: Compromising a bot could allow an attacker to manipulate its processes, such as approving fraudulent transactions."

The participants highlighted integration points, a lack of staff training, and automation workflows susceptible to cybersecurity threats. I agree with their responses, as automation technologies introduce new attack surfaces, and third-party integrations are often weak points in security.

4.3.2.2 Vulnerability

Vulnerability is a weakness or flaw in a system, process, or security framework that attackers can exploit to gain unauthorised access, disrupt operations, or compromise data integrity (Jimmy, 2024). This concerns the second interview question. Vulnerability is derived from the research question that gave rise to the first theme. While offering numerous benefits, the rapid automation technologies of processes within South African banks also introduce a new set of cybersecurity vulnerabilities. This subsection is divided based on the feedback of the ten participants.

4.3.2.2.1 Participant 1

Participant 1 (Manager, 45) discusses vulnerabilities. He said:

"I think it's transitioning from legacy to new systems. Many Traditional Banks have been transitioning from their legacy systems as part of their Digital Transformation drive to meet new customer needs and new entrants (E.g., Neo-Banks and Fintechs) and remain competitive."

He further said:

"Also, I would say they are forced to transform the bank, yet they still need to run it, and therein lies the potential threat/vulnerability, as they have to operate on two different platforms to service the same client. I believe it's forming partnerships/collaborations with third-party vendors and FinTechs. Any partnership that enhances customer experience and thus gains a competitive edge will require some form of integration into the partner's environment and vice versa."

4.3.2.2.2 Participant 2

Participant 2 (a 44-year-old South African) discussed vulnerabilities. She said the following:

"From my experience, the vulnerabilities emerging are as follows: If data access controls and encryption are weak, automated systems handling sensitive customer data may be more prone to breaches.

"Also, integrating AI with legacy systems can create security gaps and issues, as legacy systems often lack modern security measures".

She also said:

"In my experience, using third-party and cloud-hosted AI solutions can increase exposure to cybersecurity risks if external security measures aren't robust enough to prevent individuals from accessing the applications and people's banking profiles."

She concluded by saying:

"In my experience, Robotic Process Automation and Bots are often given high system access. This can be dangerous as the bots can be hijacked and utilised for unauthorised actions."

4.3.2.2.3 Participant 3

Participant 3 (Female, 44) said:

"I've seen how interrupting an automatic process can affect the flow of processes. A knowledgeable human needs to maintain data confidentiality/ availability, and integrity. Automatic technologies are helpful and efficient, but banks should not entirely rely on them."

4.3.2.2.4 Participant 4

Participant 4 (a 48-year-old South African) discussed vulnerabilities. He said:

"I would say that the confidentiality and integrity of customer data can be easily compromised if adequate safeguards are not implemented".

4.3.2.2.5 Participant 5

Participant 5 (46: Manager) spoke about vulnerabilities. He said:

"In my opinion, South African banks' automation technologies introduce cybersecurity risks, including API security risks, AI/ML model vulnerabilities, RPA bot vulnerabilities, Identity and access management weaknesses and Cloud security risks."

4.3.2.2.6 Participant 6

Participant 6 (Black/African, 50) talked about vulnerabilities. She said the following:

"From my experience, emerging vulnerabilities include AI Algorithm Manipulation, Data Storage and Transfer Risks and Legacy Systems. AI Algorithm Manipulation: Attackers may tamper with AI models to create fraudulent outcomes or bypass security checks. Data Storage and Transfer Risks: Automation increases reliance on cloud systems, which can be vulnerable to targeted attacks during data transit or storage. Legacy Systems: Integrating modern automation technologies with older systems can expose unpatched vulnerabilities."

4.3.2.2.7 Participant 7

Participant 7 (45: South African) spoke about vulnerabilities, which he said:

"From my experience, these include Phishing and Social Engineering, Data Breaches, Denial-of-Service Attacks and Ransomware Attacks."

He also said:

"Phishing and Social Engineering: Sophisticated phishing attacks and social engineering tactics can target automated systems, tricking employees or customers into divulging sensitive information. Data Breaches: Automated workflows often handle large volumes of sensitive data, making them attractive targets for cybercriminals looking to steal personal and financial information."

He further said:

"In my experience, there are also Denial-of-Service (DoS) Attacks. These attacks can overwhelm automated systems, leading to service disruptions and degraded performance. Ransomware Attacks: Financial

institutions are prime targets for ransomware attacks, which can encrypt critical data and disrupt operations until a ransom is paid."

4.3.2.2.8 Participant 8

Participant 8 (Coloured, 51) said:

> *"In my experience, automation technologies in South African banks are beneficial for streamlining processes, but they also open up a range of vulnerabilities. One big concern is the risk of poorly secured APIs, which can become gateways for attackers if not adequately monitored."*

He also said:

> *"Another issue is insider threats—automating processes can sometimes mean giving broader access to sensitive systems, and if these controls aren't tight, it's a significant risk."*

He further said the following:

> *"I've also seen how automation technology tools, like bots, can be exploited for fraud or manipulated in phishing attacks, especially if they're not constantly updated. Third-party software is reliant; if vendors aren't secure, it also becomes a risk for the bank. It's a double-edged sword—automation technologies are necessary, but it's critical to be proactive about plugging these potential security gaps."*

4.3.2.2.9 Participant 9

Participant 9 (50: Manager) talked about vulnerabilities that:

> *"From my experience, most digital banking platforms rely heavily on APIs (Application Programming Interfaces), which can introduce significant vulnerabilities if not properly configured. Issues such as insufficient access controls and unpatched software dependencies are common challenges associated with API usage. Additionally, many automation technology tools depend on third-party libraries, which, if not regularly updated, can present exploitable security risks."*

He spoke further by saying:

> *"For example, in my experience, South African banks encountered significant challenges when integrating the Home Affairs API for customer authentication, highlighting the importance of robust configuration, regular updates, and thorough security assessments for API-based solutions."*

4.3.2.2.10 Participant 10

Participant 10 (54: Male) spoke about vulnerabilities that:

> *"From my experience, automation technologies in the digital banking industry introduce specific vulnerabilities that attackers could exploit. These include risks associated with the increased complexity of systems, reliance on third-party tools, and the speed at which automated processes operate. Here are some emerging vulnerabilities specific to South African banks automating their processes:"*

He said:

> *"Firstly, I would say Vulnerabilities in Robotic Process Automation (RPA). This includes Hardcoded Credentials, Script Tampering and Insecure Communication Channels. Hardcoded Credentials: Many RPA bots are configured with embedded credentials to access various systems. If these credentials are not encrypted, they can be easily extracted. Script Tampering: Bots can be exploited if attackers gain access to the scripts, allowing them to manipulate workflows and execute unauthorised transactions. Insecure Communication Channels: Bots often communicate between systems, and without secure protocols like TLS, these communications are susceptible to interception."*

He further said the following:

> *"Secondly, I would say AI and Machine Learning Exploits. This includes Adversarial Attacks, Data Poisoning and Model Theft. Adversarial Attacks: Attackers can deliberately craft inputs to AI systems to confuse them, such as bypassing fraud detection by exploiting patterns in machine learning models. Data poisoning, which compromises the training data of machine learning systems, can skew their decision-making processes, leading to financial loss or reputational damage. Model Theft: If machine learning models are not adequately secured, attackers can reverse-engineer or steal them, gaining insights into how fraud detection or credit scoring systems work."*

He also said the following:

> *"Thirdly, I would say APIs and System Integrations. This includes Insecure APIs, Supply Chain Risks and Data Exposure. Insecure APIs: APIs that connect automated workflows can be weak if they lack strong authentication and rate-limiting measures. There are supply chain risks associated with many automation technologies that rely on third-party integrations. Compromising a vendor's system could provide access to the bank's core systems. Data Exposure: APIs might inadvertently expose sensitive data to unauthorised parties if not correctly configured."*

The responses identified AI-driven attacks, API security risks, and insider threats as key vulnerabilities. I agree with their assessment since these vulnerabilities align with known cybersecurity risks in automated banking environments.

4.3.2.3 Exploit

An exploit is a method, technique, or piece of code used by attackers to exploit a system, application, or network vulnerability to gain control, steal data, or cause damage (Aslan et al., 2023). Exploit is the third category of the first research question and relates to the third interview question. It was derived from the first theme, research question and the theoretical framework. Below are the responses from the ten participants concerning how attackers can exploit vulnerabilities in automated banking systems.

4.3.2.3.1 Participant 1

Participant 1 (45: Black/African) spoke about how attackers exploit vulnerabilities. He said:

> *"I would say, firstly, transitioning from legacy to new systems. This involves Data exposure and outdated security systems. For data exposure, sensitive client data may be exposed as the banks migrate from legacy to new systems. Outdated security systems. Most legacy systems tend to operate on old/analogue systems, which may be outdated."*

He spoke further by saying:

> *"Secondly, I would say forming partnerships/collaborations with third-party vendors and FinTechs. This involves third-party vulnerabilities, compliance, and regulatory differences. Third-party vulnerabilities: If partners have weaker security practices, attackers can exploit their systems to access the primary organisation's data or infrastructure. Compliance and Regulatory Differences: While banks are heavily regulated, these partners are not regulated to the same compliance standards, which could expose the bank to legal liabilities and security threats that attackers might exploit."*

4.3.2.3.2 Participant 2

Participant 2 (Female, 44) talked about the exploitation of vulnerabilities by saying the following:

> *"In my experience, attackers can exploit these vulnerabilities in several ways. They may exploit weak access controls to infiltrate systems handling sensitive customer data, leading to unauthorised data access, theft, or financial fraud. By targeting outdated security protocols in legacy systems, attackers can use vulnerabilities as entry points, compromising integrated AI and automation technologies processes to disrupt services or steal data."*

She also said the following:

> *"In my experience, attackers can hijack poorly secured RPA bots with high access levels, allowing them to execute unauthorised transactions, modify customer records, or extract sensitive information."*
>
> *"They can also exploit weaker security measures in third-party or cloud-hosted AI systems to access the bank's automated processes, leading to potential data leaks or system disruptions."*

4.3.2.3.3 Participant 3

Participant 3 (42: South African) spoke about attackers exploiting vulnerabilities. The manager mentioned the following:

> *"Data breach /leak and denial of service."*

4.3.2.3.4 Participant 4

Participant 4 (Male, 48) talked about the exploitation of vulnerabilities. He said the following:

> *"I believe phishing attacks and data breaches are the most prevalent forms of attacks."*

4.3.2.3.5 Participant 5

Participant 5 (46: Nigerian) said the following:

> *"In my experience, attackers can exploit vulnerabilities in automated banking systems through API Security Risks: This involves API key theft, SQL injection and Cross-Site Scripting (XSS). AI/ML Model Vulnerabilities: This involves data poisoning, model inversion, and*

evasion attacks. RPA Bot Vulnerabilities: This involves credential theft, process manipulation, data manipulation, and data exfiltration. Identify and Access Management weaknesses: privilege escalation, Identity spoofing and Session hijacking. Cloud Security Risks: this involves cloud storage breaches, misconfigured resources and unauthorised access."

The manager further said:

"In my experience, Exploitation Techniques include phishing, social engineering, network exploitation, malware injection, and insider threats. Data breaches, financial loss, reputation damage, regulatory non-compliance, and system downtime are consequences. Mitigation includes regular security audits, penetration testing, employee training, incident response planning, and continuous monitoring."

4.3.2.3.6 Participant 6

Participant 6 (Black/African, 50) said:

"I believe attackers exploit vulnerabilities through injection attacks, credential stuffing, and social engineering. Injection Attacks involve introducing malicious code into automated scripts or workflows. Credential Stuffing involves using compromised credentials to access automated systems. Social Engineering involves exploiting staff's unfamiliarity with new technologies to gain unauthorised access."

4.3.2.3.7 Participant 7

Participant 7 (45: Male) spoke about exploiters of vulnerabilities. The Black/African said the following:

"In my experience, attackers can exploit these vulnerabilities in the following ways: Phishing and social engineering, ransomware attacks, data breaches, and Denial-of-service attacks."

"For Phishing and Social Engineering: an attacker sends a seemingly legitimate email to a bank employee, tricking them into clicking a malicious link or sharing their credentials. This can grant the attacker access to the bank's internal systems."

He also said the following:

"I would also say Ransomware Attacks: An example is malware that encrypts the bank's critical data and demands a ransom for decryption. This can halt operations until the ransom is paid or the bank restores its data from backups."

“Data Breaches: An example is exploiting vulnerabilities in automated data processing systems, where attackers can gain unauthorised access to sensitive customer data, leading to identity theft and financial fraud.”

“Denial-of-Service (DoS) Attacks: An example is when attackers flood the bank's automated systems with excessive traffic, causing them to crash or become unresponsive, disrupting online banking services.”

4.3.2.3.8 Participant 8

Participant 8 (Male, 51) talked about the exploitation of vulnerabilities. The permanent staff said the following:

“In my experience, attackers can exploit these vulnerabilities in several ways, depending on the type of system and the weakness they’re targeting. For instance, they might use poor authentication mechanisms to gain unauthorised access or exploit unpatched software to inject malicious code.”

“In the case of DDoS attacks, they can use weak network security or misconfigured devices to flood systems with traffic, causing disruptions.”

He further said:

“In my experience, attackers often look for the most straightforward entry points, like outdated systems or human error, and use those to compromise sensitive data or interrupt services. It’s about finding and exploiting the weakest link in the chain.”

4.3.2.3.9 Participant 9

Participant 9 (50: Masters) said:

“In my experience, automated workflows incorporating API integrations and decision-making algorithms are common targets in the South African banking industry.”

4.3.2.3.10 Participant 10

Participant 10 (Permanent, 54) spoke about exploiters of vulnerabilities. The staff with 24 years of work experience said:

“I believe attackers can exploit vulnerabilities in automated banking processes by leveraging weaknesses in system security, configurations,

and operational practices. Here's how specific vulnerabilities in South African banks' computerised systems can be exploited:"

He said the following:

> *"Firstly, I would say that exploiting RPA vulnerabilities. This includes Credential Theft, Manipulating Workflow Scripts and Replay Attacks. Credential Theft: attackers can extract hardcoded or improperly stored credentials from bots, gaining access to banking systems and customer accounts."*
>
> *"Manipulating Workflow Scripts by tampering with automation scripts, attackers can authorise fraudulent transactions, escalate access privileges, or disable critical alerts. Replay Attacks: Intercepting and reusing communication between bots and systems can allow attackers to replicate legitimate actions for malicious purposes."*

He further said the following:

> *"Secondly, I would say that Compromising AI and Machine Learning Systems includes Data Poisoning, Adversarial Attacks, and Exfiltrating Models. Data Poisoning: Injecting malicious data into AI training datasets can skew fraud detection or credit scoring systems, enabling fraudulent activities to pass undetected."*
>
> *"Adversarial Attacks through crafting inputs to deceive machine learning algorithms (e.g., bypassing fraud checks by mimicking legitimate transaction patterns). Exfiltrating Models by stealing or reverse-engineering AI models can provide insights into decision-making logic, helping attackers identify exploitable weaknesses."*

Participants mentioned that attackers exploit weaknesses through API security risks, identity management weaknesses, and manipulate AI models. I agree with these responses because attackers frequently target these areas to breach security defences.

4.3.3 Conclusion of Proposition 1

Proposition 1: New cybersecurity threats emerge as automation technologies transform work in digital banking. The key findings were that automation technologies introduce vulnerabilities, including API security risks, adversarial attacks on AI models, and the exploitation of RPA workflows. Staff training, third-party risks, and integration points are also critical areas of concern. Automation technology-driven transformation requires proactive and robust security strategies to address these emerging threats.

4.4 Findings of Proposition 2

This includes data analysis and presenting the findings and conclusion regarding the second proposition.

4.4.1 *Data Analysis for Proposition 2*

ATLAS TI 25 and manual process were used in the data analysis. Theme 2 is the mitigation of Cybersecurity Risks obtained from the content of research question 2.

The table below, Table 4.6, is titled "Interview Questions of Theme 2."

Interview Questions as per Theme 2.

Question no.	Category	Number of questions
Q4-Q5	Organisation	2
Q4-Q5	Regulation	2
Q4-Q5	Technology	2

Table 4.6: Interview Questions of Theme 2.

Table 4.6 shows that interview question numbers Q4 and Q5 consist of three categories: Organisation, Regulation, and Technology. There are two interview questions for each category.

Below is Table 4.7, titled "Interview Schedule" according to Theme 2.

Interview Schedule as per Theme 2

Question no.	Question	Category
Q4	In your opinion, what specific cybersecurity measures or strategies can South African banks employ to mitigate the cybersecurity risks associated with increased automation technologies in the	Organisation, Regulation, Technology

	digital banking sector?	
Q5	Are new approaches for mitigation needed?	Organisation, Regulation, Technology.

Table 4.7: Interview Schedule as per Theme 2.

Table 4.7 shows the number of each interview question in Theme 2. It also states each interview question and shows the three categories associated with each question, which are Organisation, Regulation, and Technology.

We also present tables and figures in the Appendix for Theme 2. Tables 3A and 4A are in Appendix A. The Theme-Category Codebook of Theme 2 in Table 3A of Appendix A shows the second research question, the second theme, and the three categories: organisation, regulation, and technology. It also shows an example of a quotation from each category. The Category-Code Codebook of Theme 2, shown in Table 4A of Appendix A, includes the second Theme, the three categories —Organisation, Regulation, and Technology —the codes for each category, and a description of each code.

Figures 4A, 5A, and 6A are included in Appendix B. Figure 4A displays the theme 2 bar chart graph, which categorises data across ten participants. The word frequencies for Theme 2 are presented in Figure 5A of Appendix B. Figure 6A of Appendix B displays the Theme 2 network, including its categories and codes.

4.4.2 *Proposition 2*

The findings for Research Question 2 indicate that the South African digital banking industry can mitigate cybersecurity risks from automation technologies through a combination of organisational strategies, regulatory compliance, and technological advancements. Banks should implement continuous employee training, establish Chief Information Security Offices, and conduct regular security audits. Regulatory adherence, including compliance with South African data protection laws, is critical. Technologically, AI-driven threat detection,

multi-factor authentication, and zero-trust architecture must be adopted. The implication is that banks must proactively invest in cybersecurity frameworks, thereby fostering a secure and resilient banking ecosystem that addresses the evolving risks of automation.

The theme of the second research question is mitigating cybersecurity risks. This concerns the three categories derived from the second research question and the theoretical framework: Technology, Organisation, and Regulation. This subsection contains the responses of the ten participants answering interview questions 4 and 5.

The table below, Table 4.8, is titled "Theme 2" and displays categories along with the number of quotations.

Theme- Mitigation of Cybersecurity Risks	Total number of quotations
Organisation (Category)	13
Regulation (Category)	6
Technology (Category)	59

Table 4.8: Theme 2 shows categories and the number of quotations.

Table 4.8 presents the three categories in Theme 2, along with the total number of quotations for each category, as calculated using Atlas.ti 25. The 10 participants have provided the most relevant quotations below.

4.4.2.1 Organisation

An organisation is a structured entity, such as a company or institution, that coordinates people, resources, and processes to achieve specific goals, including cybersecurity risk management and mitigation (Thomas and Sule, 2023). This is another category in the second research question. It was derived from the second research question and the theoretical framework. It answers both interview questions 4 and 5. Participants 1, 4, 5, 7, 8, and 9 responded

concerning this category organisation. Participants 2, 3, 6, and 10 did not respond.

4.4.2.1.1 Participant 1

Participant 1 (45: Manager) spoke about the organisation as a measure to mitigate cybersecurity risks in responding to interview question 4. He said:

> *"Lastly, I would say Employee training—regular training for all employees. The training should be practical, with real-life scenarios, and include non-conformance implications."*

4.4.2.1.2 Participant 4

Participant 4 (48: South African) responded to interview question 5 by talking about the organisation as a new approach for mitigation, which is needed. He said:

> *"I believe so by Implementing a Chief Information Security Office to focus on cyber resilience."*

4.4.2.1.3 Participant 5

Participant 5 (Masters, 46), responding to interview question 4, spoke about the organisation. He said:

> *"I would establish robust incident response planning and invest in employee training and awareness programs."*

Also, while responding to interview question 5, he talked about the organisation and said that new approaches to mitigation are needed.

He said they are:

> *"In my experience, continuous security monitoring/incident response and cybersecurity awareness/training programs."*

4.4.2.1.4 Participant 7

Participant 7 (45: Manager) spoke about the organisation as a strategy for mitigating cybersecurity risks in automation technologies in the digital banking sector in South Africa in answering interview question 4. He said:

> *"In my experience, for regular security audits and penetration testing, frequent security assessments and penetration tests must be conducted to identify and address vulnerabilities within automated systems and third-party integrations".*

He also said:

> *"In my opinion, it also includes employee training and awareness. Train employees on cybersecurity best practices, including recognising phishing and social engineering attacks."*

And he finalised it by saying:

> *"Lastly, I would say Incident Response Planning: Develop and maintain robust incident response plans to address and mitigate the impact of cybersecurity incidents quickly."*

4.4.2.1.5 Participant 8

Participant 8 (51: Coloured) spoke about the organisation when answering question 4 of the interview. He said:

> *"I also believe that regular penetration testing and vulnerability assessments are crucial for identifying and addressing weaknesses before attackers exploit them."*

He also said:

> *"In my experience, banks should invest in advanced AI-driven threat detection systems to monitor and respond to unusual activity in real-time."*

He said:

> *"Employee training on cybersecurity, best practices and customer awareness campaigns can help reduce human error, which is often a significant vulnerability."*

4.4.2.1.6 Participant 9

Participant 9 (50: Permanent) spoke about the organisation when answering question 4 of the interview. He said:

> *"I would also say regular vulnerability assessments are included."*

The participants emphasised the importance of continuous improvement, employee training, and incident response planning to mitigate cybersecurity risks. I agree with their responses because proactive organisational measures strengthen cybersecurity resilience.

4.4.2.2 Regulation

Regulation is a set of rules, laws, or guidelines established by governments or industry bodies to ensure compliance, security, and ethical practices in sectors like banking, finance, and cybersecurity (Ridzuan et al., 2024). This is the third category of the second research question of this study. It was derived from the research question and the theoretical framework. It relates to interview questions 4 and 5. Responses regarding regulation were provided by participants 1, 5, and 8.

4.4.2.2.1 Participant 1

Participant 1 (Master's, 45) discussed regulation in addressing cybersecurity risk mitigation in response to question 4. He said:

> *"Secondly, I would say that Partners must conform to the exact compliance and regulatory standards. All bank partners should adhere to the same regulatory standards, as this will minimise external threats."*

4.4.2.2.2 Participant 5

Participant 5 (46: Black/African) spoke about regulation when addressing interview question 4. He said:

> *"In my experience, collaborative measures include Industry information sharing and threat intelligence, collaboration with cybersecurity experts and peers, Participation in cybersecurity forums and workshops,*

engagement with regulatory bodies and continuous compliance monitoring."

He also said:

"I believe the best practices are adopting ISO 27001 and the NIST Cybersecurity Framework, conducting regular security audits and penetration testing, implementing the Secure Software Development Life Cycle (SSDLC), threat modelling and attack simulation, and continuous monitoring and incident response planning."

He further said:

"I believe regulatory compliance includes adhering to South African banking regulations (e.g., POPIA), complying with international standards (e.g., PCI-DSS), conducting regular security assessments and audits, implementing regulatory requirements for AI/ML, and taking data protection and privacy measures."

Participant 5, while responding to interview question 5, spoke about regulation, in which he said:

"In my experience, emerging standards/frameworks include NIST Cybersecurity Framework 2.0, ISO 27001:2022, PCI-DSS 4.0, Cloud Security Alliance (CSA) Star certification, and Secure Controls Framework (SCF)."

4.4.2.2.3 Participant 8

Participant 8 (51-year-old male) spoke about regulation in response to interview question 4. He said the following:

"Lastly, I would say collaborating with regulatory bodies and staying ahead of compliance requirements and sharing threat intelligence with other financial institutions can strengthen the sector's overall defences against cyber risks."

The responses highlighted compliance with data protection laws, regulatory collaboration, and industry-wide security standards. I agree, as regulatory adherence ensures a structured and consistent approach to mitigating cybersecurity threats in digital banking.

4.4.2.3 Technology

Technology is the application of scientific knowledge, tools, and systems to solve problems, enhance efficiency, and improve security, particularly in fields like automation technologies, AI, and cybersecurity (Lysenko et al., 2024). Technology is a specific cybersecurity measure and strategy that South African banks can employ to mitigate the cybersecurity risks associated with the increased adoption of automation technologies in the digital banking sector. This presentation of the findings involves ten participants whose responses are listed.

4.4.2.3.1 Participant 1

Participant 1 (45: Manager), in response to interview question 4, said:

> *"Firstly, I would say a multi-layered approach is needed. Banks can adopt/implement a cyber-attack strategy that includes advanced tech like AI and ML to spot potential threats in real-time."*

In response to interview question 5, he said the following:

> *"I would say it's not necessary. Their approach needs to be tech-led. Adopting AI, ML, cloud computing and blockchain can ensure that cyber threats are minimised and tracked in real-time."*

4.4.2.3.2 Participant 2

Participant 2 (Female, 44) discusses technology when answering interview question 4. She said:

> *"In my experience, South African banks can adopt a multi-layered approach to cybersecurity to mitigate the risks associated with increased automation technologies in the digital banking sector. In my opinion, here are some targeted strategies and measures:"*

She further said:

> *"First, I would say strengthen Identity and Access Management (IAM). This involves Multi-factor Authentication (MFA), zero-trust architecture, and privileged access management. Implement MFA for customers and employees to add an extra layer of security. Employ "never trust, always verify" principles to authenticate and authorise every access request. Privileged Access Management (PAM): This policy restricts access to sensitive systems and data based on the principle of least privilege."*

The manager also said:

> *"Second, I would say enhance Endpoint and Network Security. This includes Endpoint Detection and response, Network Segmentation, and AI-powered Intrusion Detection systems. Endpoint Detection and Response (EDR): Deploy EDR solutions to monitor and respond to potential threats on connected devices. Network Segmentation: Isolate critical systems to minimise the spread of breaches or malware. AI-Powered Intrusion Detection Systems (IDS): These systems use AI and machine learning to detect and respond to anomalies in real-time."*

She lastly said:

> *"Third, I would say secure automated systems. This involves Robust API security, Bot Mitigation Tools, Code Review, and Vulnerability Scanning. Robust API Security involves using secure APIs in automated systems, which employ strong encryption, rate limiting, and input validation. Bot Mitigation Tools deploy tools to differentiate between legitimate automation and malicious bots. Code Review and Vulnerability Scanning regularly audit automated scripts and processes for vulnerabilities."*

Responding to interview question 5, the 17-year work experience manager said:

> *"I believe yes. Some ways in which new approaches for mitigation are needed are as follows: The banks are exploring the use of AI to monitor and detect anomalies in real-time. This can help identify unusual patterns across automated workflows and spot potential threats early."*

She further said the following:

> *"In my experience, the Zero Trust model also requires strict user and device identity verification. This reduces the risk of unauthorised access within automated and legacy-integrated systems."*
>
> *"For RPA bots, the banks are adopting role-based access control and regular security audits that limit their access scope, reducing the impact of potential hijacking."*

4.4.2.3.3 Participant 3

Participant 3 (a 42-year-old South African) spoke about the mitigation strategy for cybersecurity risks in the context of technology. While responding to interview question 4, she said:

> *"I would say educated personnel, zero trust, end-to-end encryption, and detection/monitoring tools."*

When answering interview question 5, Participant 3 said:

"I believe yes. To continuously assess the effectiveness of current approaches and follow technological advancement trends to implement the most effective tools for assistance."

4.4.2.3.4 Participant 4

Participant 4 (48: Male), in responding to interview question 4, said:

"I would say that implementing a zero-trust capability will ensure improved cyber resilience."

4.4.2.3.5 Participant 5

Participant 5 (Masters, 46) said while responding to interview question 4 that:

"In my experience, to mitigate cybersecurity risks associated with automation technologies, South African banks can employ the following: Strategic Measures: Conduct thorough risk assessments and vulnerability scanning."

He said:

"I would implement Zero Trust Architecture and continuously monitor and analyse automated workflow activity."

Participant 5 said the following:

"In my experience, technical measures include API security gateways, multi-factor authentication (MFA) and secure-by-design principles for AI/ML models."

He also said the following:

"In my experience, Automation-Specific Measures include implementing Robotic Process Automation (RPA) security frameworks, monitoring RPA bot activity and logs, using secure data storage and processing for AI/ML models and using explainable AI (XAI) for transparency."

Participant 5, while responding to interview question 5 on technology as a category, said the following:

"I would say yes. New mitigation approaches are required. In my experience, these include AI-powered security, Zero Trust Architecture/Micro-Segmentation, and Advanced Threat Modelling/simulation."

He said the following:

"In my experience, innovative technologies include blockchain-based security, Quantum computing-resistant cryptography and AI-powered incident response."

4.4.2.3.6 Participant 6

Participant 6 (Degree, 50) discussed technology as a strategy for mitigating cybersecurity risks in response to interview question 4. She said the following:

"In my opinion, key strategies include Zero-Trust Architecture, End-to-end Encryption, Dynamic Authentication Mechanisms, and Regular Audits.

"Zero-trust architecture continuously verifies all devices and systems instead of granting default trust. Dynamic Authentication Mechanisms implement biometrics and multi-factor authentication (MFA). Regular audits, penetration testing, and security evaluations are conducted to detect vulnerabilities."

Answering interview question 5 concerning technology as a category, she said the following:

"I would say yes. Traditional defences are often insufficient. Banks must adopt AI-driven threat Detection, Blockchain-Based Validation, and Behavioural Analytics.

"AI-Driven Threat Detection: Machine learning is used for real-time monitoring and anomaly detection. Blockchain-Based Validation: Enhance transaction integrity with decentralised validation mechanisms. Behavioural Analytics: Detect unusual activity by monitoring user and system behaviour."

4.4.2.3.7 Participant 7

Participant 7 (45-year-old male) spoke about technology as a strategy for mitigating cybersecurity risks when responding to question 4. He said:

"In my experience with Advanced Threat Detection Systems, I deploy sophisticated systems that use AI and machine learning to identify and respond to unusual activities and potential threats in real-time."

He also said:

"In my experience with Multi-Factor Authentication (MFA), I implement MFA across all systems and processes to provide an extra layer of security beyond just usernames and passwords."

The participant 7 manager also said:

"In my experience, Data Encryption and Secure Storage ensure that sensitive data is encrypted both in transit and at rest and that secure storage solutions are used to protect against data breaches."

Participant 7, while responding to interview question 5 regarding technology, said:

"I would say yes. These can be done through Zero-Trust Architecture, Behavioural Analytics, and Secure Access Service Edge. Zero-trust architecture assumes external and internal threats. It involves continuously verifying the identity and integrity of users and devices, regardless of their location within or outside the network."

The manager further said:

"I would also say that behavioural analytics involves implementing AI systems to analyse user behaviour. This can help detect anomalies indicating a security breach, such as unusual transaction patterns or login times."

4.4.2.3.8 Participant 8

Participant 8 (Coloured, 51) discussed technology in response to interview question 4. He said:

"In my experience, South African banks should prioritise implementing robust multi-factor authentication systems to secure customer accounts and ensure end-to-end encryption for all digital transactions to protect sensitive data."

He also said:

"In my experience, banks should invest in advanced AI-driven threat detection systems to monitor and respond to unusual activity in real-time."

While responding to interview question 5 concerning technology, he said the following:

"I think new approaches for mitigation are needed, especially considering how quickly threats and challenges evolve in the digital banking industry.

Traditional methods can't always keep up with the sophistication of new attacks or the complexities of emerging technologies. For example, attackers constantly find ways to bypass existing defences in cybersecurity, so staying ahead requires innovative strategies and tools."

He also said:

"In my experience, similarly, in AI adoption for digital banks and telcos, mitigation isn't just about managing risks and addressing gaps like skills shortages and ethical concerns, which demand fresh perspectives. It's about being proactive, not reactive, which means rethinking how we approach problems."

4.4.2.3.9 Participant 9

Participant 9 (Black/African, 50) said the following while responding to interview question 4 concerning technology as a strategy to mitigate cybersecurity risks:

"In my experience, South African banks should adopt a multi-layered security approach to mitigate cybersecurity risks associated with increased automation technologies in digital banking. This includes implementing robust API security measures such as token-based authentication and encryption. Banks should enforce strict access controls through role-based permissions and multi-factor authentication to minimise unauthorised access."

While responding to interview question 5, participant 9 said:

"I would say yes. New approaches are needed to effectively mitigate emerging cybersecurity risks associated with automation technologies in the banking sector. Traditional measures often fail to address the sophisticated tactics attackers use targeting automation technologies."

4.4.2.3.10 Participant 10

Participant 10 (54, South African) spoke about technology when answering question 4 of the interview. He said:

"In my experience, to mitigate the cybersecurity risks associated with increased automation technologies, South African banks should adopt a multi-layered security approach that combines advanced technologies, strict governance, and continuous monitoring. Here are specific cybersecurity measures and strategies:"

He further said the following:

"Firstly, I would say that Secure Robotic Process Automation (RPA) includes encrypting credentials, limiting Bot Privileges, and ensuring script integrity. Encrypt Credentials: Store bot credentials in secure vaults, not in scripts, and use encryption for transmitting sensitive data. Limit Bot Privileges: Implement the principle of least privilege for bots, ensuring they can access only the resources required for their tasks. Script Integrity: Use version control and digital signatures to ensure automation scripts are not tampered with."

Participant 10 concluded by saying that:

"Secondly, I would say that AI and Machine Learning Defences should be strengthened. This includes Adversarial Testing, Secure Training Data, and Model Encryption. Adversarial Testing: Regularly test AI models against adversarial inputs to identify and patch vulnerabilities. Secure Training Data: Protect training datasets from manipulation by implementing strict access controls and performing integrity checks. Model Encryption: encrypt AI models to prevent theft and reverse engineering."

Participant 10, when responding to interview question 5, discussed technology and new approaches for mitigation, which are necessary. He said:

"I would say yes. New approaches to cybersecurity mitigation are needed to address the evolving risks introduced by automation technologies in the digital banking sector. Traditional cybersecurity strategies often fail to account for the unique dynamics of automated workflows, AI systems, and real-time decision-making processes. Here's why and how new approaches can make a difference:"

Participant 10 further responded by saying the following:

"First, I would say the complexity of automation technology ecosystems: Automation technologies involve interconnected systems, such as AI models, APIs and Third-party integrations."

He also said:

"Secondly, I would say the speed and scalability of attacks: automation technologies enable attackers to execute faster and more sophisticated attacks, such as using bots to mimic legitimate workflows or bypass fraud detection in real-time.

He added the following:

"Thirdly, I would say it is the emergence of new threat vectors: Advanced threats like adversarial AI attacks, supply chain vulnerabilities and

automated exploitation of insecure APIs demand novel mitigation strategies."

Participants focused on AI-powered security, API protection, zero-trust models, and blockchain solutions to enhance cybersecurity. This implies that leveraging advanced automation technologies is crucial for effectively combating evolving cyber threats.

4.4.3 *Conclusion of Proposition 2*

Proposition 2: Automation technologies can enhance operational efficiency and mitigate cybersecurity risks. The key findings include risk mitigation strategies such as adopting advanced automation technologies like AI and blockchain, implementing zero-trust security models, and adhering to regulatory frameworks. Emphasis on employee training and robust incident response mechanisms is also highlighted. The conclusion is that South African banks can proactively address cybersecurity threats while improving efficiency by leveraging cutting-edge technologies and fostering regulatory compliance.

4.5 Findings of Proposition 3

This includes data analysis, presenting the findings, and drawing a concluding proposition. This addresses the third research question, which forms the basis for the conclusions presented in this section. Two categories derived from the third research question are skills and education. These two categories were derived from the research question and the theoretical framework. The findings of Proposition 3 answer interview questions 6, 7, and 8. This section discusses the answers to interview questions 6, 7, and 8.

4.5.1 *Data Analysis of Proposition 3*

Data analysis was done manually and through ATLAS.ti 25. Theme 3 was derived from the third research question. Theme 3 is the impact of Skills Gaps on Cybersecurity Professionals.

Table 4.9 below is titled "Interview Questions about Theme 3."

Interview Questions as per Theme 3.

Question no.	Category	Number of questions
Q6	Skills	1
Q7-Q8	Education	2

Table 4.9: Interview Questions about Theme 3

Table 4.9 lists Q6 as the interview question number for the category "Skills," with a single interview question. It also shows that Q7 and Q8 belong to the category Education, and that the number of interview questions for Education is 2.

The table below, Table 4.10, is named the interview schedule as per Theme 3.

Interview Schedule as per Theme 3

Question no.	Question	Category
Q6	With the rapid adoption of digital banking automation technologies in South Africa, what new cybersecurity skill sets do you see becoming essential for professionals in this field? How will these skills differ from the traditional cybersecurity skillset?	Skills
Q7	Given the widening skills gap anticipated with the automation technologies of digital banking processes in South Africa, what strategies can be implemented to bridge this gap?	Education
Q8	Should the focus be on retraining existing	Education

	professionals or attracting new talent with specialised skills?	

Table 4.10: Interview Schedule as per Theme 3.

Table 4.10 above shows the number and category of each interview question.

We also present tables and figures of Theme 3 in the Appendix. Tables 5A and 6A are in Appendix A. The Theme-Category Codebook of Theme 3, presented in Table 5A of Appendix A, outlines the third research question, the third Theme, and the two categories of the third Theme: Education and Skills, along with an example for each category. The Category-Codes Codebook of Theme 3, as shown in Table 6A of Appendix A, presents the third Theme, its two categories —Education and Skills —the codes for each category, and a description of each code.

Appendix B contains Figures 7A, 8A, and 9A. The first figure, Figure 7A, presents a bar chart of Theme 3, with categories across ten participants. The second figure, Figure 8A, shows the word frequencies for theme 3. The third figure, Figure 9A, illustrates the network of theme 3, including its categories and codes.

4.5.2 *Proposition 3*

The findings for Research Question 3 highlight that identifying cybersecurity risks in digital banking automation technologies exacerbates the cybersecurity skills gap in South Africa. Rapid AI, machine learning, and automation technologies adoption require specialised skills in securing APIs, cloud environments, and RPA security. However, the current workforce lacks these expertise areas, creating a demand for upskilling and specialised education programs. The implication is that banks must invest in continuous training, partnerships with academic institutions, and recruitment of cybersecurity talent to bridge the gap, ensuring a resilient banking sector that can effectively address evolving cybersecurity threats.

The responses of the ten participants, numbered from 1 to 10, are discussed here. They discuss skills and education as the skills gap impacts cybersecurity professionals. The theme of the third research question is the impact of skills gaps on cybersecurity professionals.

The table below, Table 4.11, is titled "Theme 3," listing each category and the corresponding number of quotations.

Theme- Impact of Skills Gaps on Cybersecurity Professionals	Total number of quotations
Skills (Category)	32
Education (Category)	48

Table 4.11: Theme 3 with each category and number of quotations.

Table 4.11 presents the two categories in Theme 3, "Skills and Education," along with the total number of quotations derived from the Atlas. ti 25. The 10 participants listed the most relevant quotations below in the Skills and Education section.

4.5.2.1 Skills

Skills are the expertise, knowledge, and abilities required to perform specific tasks, including technical competencies in cybersecurity, risk management, and digital banking security (Kumah et al., 2024). Skills are a category in the third research question. A theme was first derived from the research question. The rapid adoption of digital banking automation technologies in South Africa has shifted the required cybersecurity skillset. Here, the participants discussed some new skills that are becoming essential in cybersecurity professionals. These new skills differ from traditional cybersecurity skills because they require a deeper understanding of emerging automation technologies and their associated risks. Traditional skills, such as network security, incident response, and vulnerability assessment, remain essential, but they must be complemented by these new skills to protect digital banking systems effectively. This skills category answers the interview question 6.

4.5.2.1.1 Participant 1

Participant 1 (45, South African) spoke about new skills becoming essential for cybersecurity professionals in response to interview question 6. The manager said:

> *"I would say it requires understanding new technologies. This will help current risk managers and regulators understand threats and how to address them."*

4.5.2.1.2 Participant 2

Participant 2 (Female, 44) said the following:

> *"I believe the new cybersecurity skill sets essential for professionals in this field are Expertise in securing AI models, understanding threats like data poisoning, and developing defences against adversarial attacks. Banks increasingly use cloud-based AI solutions, so skills in cloud infrastructure security, multi-cloud environments, and securing cloud-native applications are essential. Data lifecycle management, privacy compliance, and governance for automated and AI-driven data handling are crucial as banks house customer-related data. Identity and access management skills across diverse computerised systems are also key."*

4.5.2.1.3 Participant 3

Participant 3 (42: Black/African) spoke about new skills becoming essential for cybersecurity professionals while answering interview question 6. She said:

> *"I would say regulation compliance, entry points security, digital network security, ethical hacking, etc."*

4.5.2.1.4 Participant 4

Participant 4 (Male, 48) said:

> *"From my experience, Critical skills, including knowledge of cybersecurity frameworks like NIST CSF, data loss prevention, and email security, are required, in my opinion."*

4.5.2.1.5 Participant 5

Participant 5 (46: Male) responded to interview question 6 about new skills becoming essential for cybersecurity professionals. He said the following:

"In my experience, new cybersecurity skill sets will become essential with digital banking automation in South Africa. These include Essential New Skill Sets: Cloud Security Expertise, Artificial Intelligence/Machine Learning Security, DevSecOps/Secure Software Development Life Cycle (SSDLC), Identity and Access Management (IAM), API Security and Quantum Computing-Resistant Cryptography."

The manager further said:

"In my experience, differences from the Traditional Cybersecurity Skillset include a Shift from perimeter-based security to data-centric security, Increased focus on automation, AI/ML, and cloud security, more emphasis on DevSecOps, continuous integration, and delivery; there is a greater need for threat intelligence, incident response and analytics. Expanded skill set to include programming languages (e.g., Python, Java), Integration of IT and OT (operational Technology) security and understanding of emerging technologies (e.g., blockchain, IoT)."

He rounded up by saying:

"In my experience, Recommended Training and Certifications include CompTIA Cloud+, AWS Certified Security – Specialty, Microsoft Certified: Azure Security Engineer Associate, Certified Information Systems Security Professionals (CISSP), Certified Ethical Hackers (CEH), Certified Cloud Security Engineer (CCSE) and Certified DevSecOps Engineer (CDOE). Soft skills include communication and collaboration, problem-solving and analytical thinking, adaptability and continuous learning, business acumen, understanding of banking regulations, and leadership and management. South African cybersecurity professionals should develop these skills to address emerging threats and protect digital banking automation technologies systems."

4.5.2.1.6 Participant 6

Participant 6 (50: Manager) responded to interview question 6 by saying the following:

"I believe essential skill sets include AI and Machine Learning Expertise, Threat Intelligence Analysis, Secure DevOps and Cyber-Physical Systems Security."

"AI and Machine Learning Expertise: For securing AI-driven systems. Threat Intelligence Analysis: Advanced skills to detect and respond to automation-specific threats."

"Secure DevOps (DevSecOps): Integrating security into development cycles."

"Cyber-Physical Systems Security: Protecting systems that bridge digital and physical operations, like automated ATMs. These skills differ from traditional ones, emphasising proactive defence mechanisms and advanced technological integration."

4.5.2.1.7 Participant 7

Participant 7 (Male, 45) spoke concerning new skills becoming essential while answering interview question 6. He said the following:

"In my experience, the new cybersecurity skill sets that are becoming essential for professionals in this field are AI and Machine Learning, Cloud Security, Data Privacy and Protection, and Secure Software Development.

"AI and Machine Learning: understanding how to develop, implement, and secure AI and machine learning models is crucial. This includes knowing how to detect and mitigate adversarial attacks on these models."

He further said the following:

"In my experience, others are as follows: Cloud Security concerns proficiency in securing cloud environments, including knowledge of cloud service configurations, access controls, and compliance with cloud security standards."

"Data Privacy and Protection relates to expertise in privacy laws, regulations, and techniques for protecting sensitive data in transit and at rest."

4.5.2.1.8 Participant 8

Participant 8 (Male: 51) said the following while responding to interview question 6 concerning new skills becoming essential for cybersecurity professionals and how they differ from the traditional cybersecurity skillset:

"With digital banking automation technologies taking off in South Africa, I think cybersecurity professionals will need to focus on skills like securing APIs, understanding AI-driven threat detection and safeguarding robotic process automation (RPA) workflows. Traditional cybersecurity training didn't always prioritise these areas."

The manager further said:

"In my experience, foundational skills like penetration testing and network security are still crucial. The shift toward cloud-based systems and automated processes means we'll also need expertise in securing

DevOps pipelines, managing identity and access in increasingly complex systems, and utilising AI tools to identify anomalies proactively. In this fast-moving, highly digital environment, it's less about reacting to attacks and more about anticipating them."

4.5.2.1.9 Participant 9

Participant 9 (50: Masters) said the following while responding to interview question 6:

> *"In my experience, most automation technologies systems are hosted in the cloud, so knowledge of cloud security, particularly in securing Infrastructure-as-Code (IaC), is essential."*
>
> *"Additionally, expertise in securing APIs, AI-driven systems, and Robotic Process Automation (RPA) is crucial."*

4.5.2.1.10 Participant 10

Participant 10 (Manager, 54) said concerning skills while responding to interview question 6:

> *"I believe the rapid adoption of digital banking automation technologies in South Africa necessitates the evolution of cybersecurity skill sets. Professionals must adapt to address the complexities of automation, AI, and interconnected systems. These new skill sets will complement and sometimes differ from traditional cybersecurity capabilities."*

Participant 10 also said:

> *"In my experience, the emerging Essential Cybersecurity skill sets are: Firstly, through AI and Machine Learning Security Expertise. Key Skills relate to understanding AI and ML algorithms, particularly those used in fraud detection and customer analytics; identifying vulnerabilities in AI models, such as adversarial attacks and data poisoning; and designing secure machine learning pipelines. This is needed because banks rely on AI for decision-making. Securing these models against manipulation is crucial."*

He concluded by saying:

> *"Secondly, I would say through RPA and Automation Security. Key skills include knowledge of RPA platforms like UiPath, Blue Prism, and Automation, securing bot credentials, ensuring the integrity of automation scripts, and understanding how bots interact with banking systems and APIs. This is needed because the increasing use of bots in banking introduces new attack vectors that require specialised security knowledge."*

The participants emphasised the importance of expertise in AI security, API protection, cloud security, and DevSecOps to address the evolving threats in digital banking. This implies that these skills align with the industry's growing reliance on automation technologies and AI-driven processes.

4.5.2.2 Education

Education involves acquiring knowledge, training, and skills through formal institutions, certifications, or self-learning to develop expertise in cybersecurity and digital transformation (Atatsi, 2024). Education is the second category in the third research question, which falls under the theme of the third research question. Education is a skills gap that impacts cybersecurity professionals. Interview questions 7 and 8 fall under the Education category. Interview question 7 addresses strategies implemented to bridge the skills gaps. Interview question 8 addresses the focus: retaining existing professionals or attracting new talent with specialised skills. The ten participants responded to the educational answers to the interview questions 7 and 8.

4.5.2.2.1 Participant 1

Participant 1 (45: Male) said concerning education, which is a strategy implemented to bridge the skills gaps in responding to interview question 7:

> *"First, I would say develop targeted training programs. Banks can work with regulatory partners to create specialised training."*

He also said:

> *"Second, I would say to form strategic partnerships with educational partners. Banks can form strategic alliances with educational institutions to develop curricula that align with industry needs."*

Participant 1 further said:

> *"Third, I would say collaborate between banks. Forming forums and other networking initiatives where industry professionals and companies can share knowledge about best practices, challenges, and solutions related to automation technologies will foster a culture of learning and adaptation within the sector."*

Participant 1, while responding to interview question 8, which is about retaining existing professionals or attracting new talent with specialised skills, said:

> *"From my experience, the focus should be on both. Retain: Existing professionals possess valuable institutional knowledge and expertise that can be beneficial in navigating the complexities of automation technologies. Thus, by retaining them, banks can enhance their workforce's skills while retaining this knowledge base. Retraining existing employees is more cost-effective than recruiting new talent."*

Participant 1 further said:

> *"I would say this can help a bank reduce recruitment costs and minimise the onboarding time for new hires. Offering existing professionals opportunities demonstrates a commitment to employee development, which can boost morale and job satisfaction. New talent helps to access specialised skills. Attracting new talent with expertise in AI, ML, and cybersecurity is critical for banks to remain competitive and innovative, offering diverse perspectives on problem-solving. New talent can bring new and fresh ideas and perspectives that can drive innovation within the bank."*

4.5.2.2.2 Participant 2

Participant 2 (South African, 44), while responding to Interview Question 7 about strategies implemented to bridge the skills gap, discussed various aspects of education. She said the following:

> *"In my opinion, the strategies that can be implemented to bridge the skills gap anticipated with automated digital banking technologies are as follows: Collaborate with government agencies to fund and support cybersecurity initiatives to train individuals in advanced digital banking security."*

> *"Industry-government partnerships can help streamline and scale efforts to meet sector-wide needs—industry-driven initiatives to drive cyber-related training and upskilling.*

Participant 2, responding to interview question 8, discusses the focus on retaining and attracting new talent in education. She said:

> *"I would say the answer to this is twofold. The bank I work for is doing both. They constantly upskill individuals to keep up with international trends in cybersecurity and add new professionals to enhance the organisation's skillset."*

4.5.2.2.3 Participant 3

Participant 3 (42-year-old female) spoke about education, which consists of strategies implemented to bridge the skills gaps in cybersecurity professionals, while responding to Interview Question 7. She said the following:

> *"I believe in training and development and collaboration between educational institutions."*

Participant 3, while responding to interview question 8, said:

> *"In my opinion, both. Upskill current and attract new talent."*

4.5.2.2.4 Participant 4

Participant 4 (Manager, 48) spoke about education when responding to Interview Question 7, which concerns strategies to bridge the skills gap. He said:

> *"I believe MICTSETA must develop new Occupational Qualifications to meet the demand for cybersecurity skills."*

While responding to interview question 8, Participant 4 said both should be done to retain existing professionals or attract new talent with specialised skills. He said:

> *"I believe the focus should be on retraining and attracting new talent."*

4.5.2.2.5 Participant 5

Participant 5 (46, Nigerian) spoke about education while answering question 7 of the interview, which inquired about strategies implemented to bridge the skills gaps in cybersecurity professionals. He said:

> *"In my experience, this involves bridging the Cybersecurity Skills Gap in Digital Banking, which includes the following: Short-Term Strategies: training existing staff, hiring experienced professionals, partnerships with training providers, internship and mentorship and online courses and certifications."*

He also said:

"In my experience, long-term strategies include developing university programs, collaborating with industry associations, establishing apprenticeships, and encouraging STEM education and cybersecurity awareness programs. Industry-led Initiatives include cybersecurity boot camps, Hackathons, Industry-specific training, knowledge-sharing platforms, and international collaborations."

He further said the following:

"In my experience, this also includes government support, such as funding for cybersecurity education, a national cybersecurity strategy, tax incentives, regulatory support, and public-private partnerships.

"It also includes Talent Acquisition and Retention, which include Competitive salaries and benefits, Career development opportunities, Flexible work arrangements, Diversity and inclusion initiatives, and Employee recognition and rewards."

"By implementing these strategies, South African digital banking professionals can bridge the cybersecurity skills gap and address emerging threats."

Participant 5, while responding to interview question 8, said:

"From my experience, addressing the Cybersecurity Skills Gap involves a Two-Pronged Approach. Retrain Existing Professionals (60-70% of total talent), which involves leveraging existing knowledge and expertise, and is both cost-effective and quick to deploy. Attract New Talent (30-40% of total talent), which involves bringing fresh perspectives and specialised skills, supporting business growth, and diversifying the workforce."*

He further said:

"In my experience, key considerations include Business objectives and growth plans, skills gaps and workforce demographics, Industry trends and emerging technologies, budget and resource allocation, and talent market conditions. Optimal outcomes include a continuous learning culture, knowledge sharing, mentorship and a balanced workforce with diverse skills and expertise. This approach effectively addresses the cybersecurity skills gap, leveraging existing strengths while injecting new talent and ideas."

4.5.2.2.6 Participant 6

Participant 6 (50: Female) spoke about education while responding to interview question 7, which addresses strategies implemented to bridge the skills gaps in cybersecurity professionals. She said the following:

"In my experience, these strategies include retraining existing staff, attracting new talent, and developing knowledge partnerships. Retraining Existing Staff: Upskilling teams with AI and cybersecurity automation technologies certifications. Attracting New Talent: Collaborating with universities and tech hubs to recruit specialised talent. Knowledge Partnerships: Partnering with cybersecurity firms for training and resource sharing."

Participant 6, while responding to interview question 8, which addresses retaining existing professionals or attracting new talent with specialised skills, said:

"From my experience, a hybrid approach is recommended. Retraining ensures continuity while attracting new talent and injecting fresh expertise and innovation into the workforce."

She also said:

"Case Study from my experience: During a project with a leading South African bank, I oversaw the development and deployment of an automated fraud detection system. The system leveraged machine learning to identify anomalous transactions in real-time. One of the primary challenges was securing the AI model against adversarial attacks, where malicious actors attempted to manipulate the input data to bypass detection."

Participant 6 further said:

"To address this, we implemented Robust Data Encryption, which ensures data integrity and confidentiality. We also implemented AI Model Monitoring, which involves regularly evaluating the model's performance to identify and patch vulnerabilities. Comprehensive Staff Training was also implemented, including education on securing AI-driven systems. This approach reduced the bank's fraud rate and improved customer trust in automated processes."

4.5.2.2.7 Participant 7

Participant 7 (45-year-old male) spoke about education while responding to Interview Question 7, which addresses strategies implemented to bridge the skills gaps of cybersecurity professionals. He said:

"From my experience, the strategies to be implemented to bridge this gap are partnerships with educational institutions, upskilling and reskilling

programs, online learning platforms, and investments in technology infrastructure.

"Partnerships with Educational Institutions: Collaborate with universities, colleges, and technical schools to develop specialised curricula that align with the industry's needs. This includes internships, apprenticeships, and hands-on training programs."

Participant 7 also said the following:

"In my experience, others are upskilling and reskilling programs, which invest in continuous learning and development programs for existing employees to update their skills with the latest technologies and practices."

"Online Learning Platforms: Utilise online learning platforms like Coursera, Udemy, and LinkedIn Learning to provide accessible and affordable training in digital skills."

"Investment in Technology Infrastructure: Ensure educational institutions and training centres have access to the latest technology and infrastructure to provide hands-on experience with digital banking tools."

Participant 7, while responding to interview question 8, which is about retaining existing professionals or attracting new talent with specialised skills, said:

"In my experience, both approaches are crucial and complement each other in addressing the skills gap because you must strike a balance in the workforce. This will not involve a system or process overhaul but an enhancement."

He also said:

"In my experience, Retraining Existing Professionals: Leverage Experience: Current employees have valuable industry knowledge and experience. Retraining them in new automation technologies ensures that this expertise is not lost. Cost-Effective: Retraining can be a more cost-effective alternative to hiring and onboarding new talent. Employee Retention: Providing opportunities for growth and development helps retain valuable employees, reducing turnover."

The permanent staff manager went further to say:

"In my experience, when attracting new talent with specialised skills and fresh perspectives, new talent brings fresh ideas and innovative approaches, which can be vital for adapting to rapidly changing technologies. Hiring individuals with specialised skills can address immediate gaps that cannot be quickly filled through retraining. Also, diverse skill sets involve attracting diverse talent pools that can introduce

varied skill sets and perspectives, enhancing the bank's overall capabilities."

4.5.2.2.8 Participant 8

Participant 8 (51: Degree) spoke about education when answering question 7 of the interview, which inquired about strategies to bridge the skills gap. He said the following:

> *"In my experience, the skills gap in South Africa's digital banking sector can be addressed by focusing on upskilling and reskilling initiatives accessible to everyone, especially those already in the workforce."*
>
> *"We need more partnerships between banks, tech companies, and educational institutions to offer affordable or even free training programs tailored to the specific tools and systems used in the industry."*

Participant 8 further said:

> *"I'd also say mentorship programs and internships could significantly contribute to giving people hands-on experience. Additionally, let's not forget to promote digital literacy at the grassroots level—starting with schools and community programs — to build a pipeline of tech-savvy talent early on. This needs to be backed by government policies encouraging skills development and investment in automation technologies."*

Participant 8 responded to interview question 8, which is about retaining existing professionals or attracting new talent with specialised skills (under education), by saying:

> *"In my experience, the focus should be on a balanced approach—retraining existing professionals while attracting new talent with specialised skills. Retraining is excellent because it builds on the experience and knowledge of those who already understand the organisation and its culture, which can be a huge advantage."*

He said:

> *"At the same time, I believe bringing in fresh talent with expertise in specialised areas, especially in emerging fields like AI or advanced cybersecurity, injects new ideas and perspectives that can drive innovation. A mix of both strategies would help organisations adapt to new challenges while still valuing and leveraging the experience of their current workforce."*

4.5.2.2.9 Participant 9

Participant 9 (50: Manager) discussed interview question 7, which pertains to education strategies implemented to bridge the skills gaps of cybersecurity professionals. He said:

> *"From my experience, to bridge the widening skills gap in South Africa's digital banking sector, banks can implement a combination of targeted training programs, partnerships with educational institutions, and internal talent development initiatives. Offering specialised certifications in emerging automation technologies such as AI, cloud security, and automation technologies tools (like RPA) can help upskill the workforce."*

Participant 9 also responded to interview question 8, which is about education as well and said:

> *"I believe the focus should be on a balanced approach that includes retraining existing professionals and attracting new talent with specialised skills. Retraining current employees ensures they can adapt to evolving technologies and cybersecurity challenges, leveraging their industry experience and understanding of the bank's systems."*

4.5.2.2.10 Participant 10

Participant 10 (54-year-old male) spoke about education in response to interview question 7, regarding strategies implemented to bridge the skills gaps in cybersecurity professionals. The manager said:

> *"I would say bridging the skills gap in South Africa's digital banking sector, particularly in cybersecurity for automation technologies, requires a multi-faceted approach. Here are strategies to address this gap effectively:"*

He also said the following:

> *"Firstly, I would say that this can be done through upskilling and reskilling the existing workforce. This Includes Targeted Training Programs, on-the-job training, and micro-certifications. Targeted training programs offer specialised courses on RPA security, AI governance, API management, and advanced analytics. Leverage platforms like Coursera, edX, and Udemy for flexible, self-paced learning."*
>
> *"On-the-Job Training: Implement apprenticeship programs where employees can work alongside automation technologies and cybersecurity experts to gain hands-on experience. Micro-Certifications: Promote quick, targeted certifications (e.g., in AI security, API*

management) that allow professionals to build relevant skills incrementally."

He further said the following:

"Secondly, I would say it is done through collaboration with educational institutions. This includes industry-academic partnerships and the incorporation of automation technologies into IT and cybersecurity degrees. Industry-Academic Partnerships: Partner with universities and technical colleges to develop curricula tailored to the cybersecurity needs of automated banking systems."

"Sponsor research projects and internships focused on cybersecurity innovations in automation technologies. Incorporate Automation Technologies into IT and Cybersecurity Degrees: Encourage the inclusion of RPA, AI security, and API management modules in existing IT and cybersecurity programs."

Participant 10 responded to interview question 8, also about education in retaining and attracting by saying:

"In my experience, addressing the cybersecurity skills gap in South Africa's digital banking sector requires retraining existing professionals and attracting new talent with specialised skills. However, the emphasis on each approach depends on the organisation's current workforce capabilities, the urgency of skills demand, and long-term sustainability goals."

He further said the following:

"I would, therefore, say a Balanced Approach is required. For the Short Term (1–2 Years), emphasise retraining. Leverage your existing workforce to address skill gaps quickly. Build foundational knowledge in automation technologies and cybersecurity among current employees. Ensure continuity by enhancing the expertise of trusted team members. Attracting new talent for the medium to long term (3+ years) is essential."

"Focus on specialised recruitment to bring expertise in advanced systems and innovation. Build partnerships with educational institutions to create a talent pipeline. Develop structured mentorship programs where new talent and experienced staff collaborate."

The responses emphasised collaborative efforts between banks, educational institutions, and regulatory bodies to bridge the cybersecurity skills gap through training programs, certifications, and government initiatives. This result demonstrates that a multifaceted approach, combining upskilling and new talent acquisition, is essential for addressing cybersecurity workforce shortages.

4.5.3 *Conclusion of Proposition 3*

Proposition 3: The rapid growth of automation technologies will impact the cybersecurity skills gap. Key findings were that the skills gap is widening due to the need for AI model security, API protection, and cloud security expertise. Strategies to address this gap include retraining existing professionals, attracting new talent, and collaborating with educational institutions to develop targeted curricula. The conclusion is that bridging the skills gap requires a dual approach of upskilling current employees and recruiting specialists to meet the demands of a rapidly evolving digital banking landscape.

4.6 Summary of the findings

Cybersecurity Threats in automation technologies introduce risks such as adversarial AI attacks, RPA vulnerabilities, and API security issues. Mitigation Strategies involve leveraging advanced automation technologies, regulatory compliance, and employee training, which are crucial for resilience. Skills Gaps include addressing the gap, which requires targeted education initiatives and a balance of retraining and recruitment strategies. The study emphasises the importance of a multifaceted approach to ensure security, efficiency, and workforce readiness in South Africa's digital banking sector.

Suggested improvements are discussed as follows. Frame these challenges using OB constructs such as: Cognitive and emotional resistance, Lack of psychological safety and role ambiguity in technology transitions. This provides depth to the “human angle” in cybersecurity and aligns with the original research problem statement. Position cybersecurity resilience as a function of transformational leadership, linking leaders’ communication and empowerment style to the adoption of new tools, employee engagement in security awareness and the integration of cybersecurity into organisational strategy. Integrate COBIT or ISO governance principles into the conceptual framework to demonstrate how clear accountability, performance metrics, and risk management practices can support the adoption of cybersecurity automation technologies.

CHAPTER 5. DISCUSSION OF THE FINDINGS

5.1 Introduction

This chapter presents the demographic profile of ten respondents and discusses Propositions 1, 2, and 3. Proposition 1 includes interview questions 1, 2, and 3. Proposition 2 provides interview questions 4 and 5. Proposition 3 includes interview questions 6, 7, and 8. Finally, the conclusion is included.

5.2 Demographic profile of respondents

These include the code, which is the number the participants carry; the gender, which is either male or female; the nationality, which is South African, Nigerian, and UAE; the race, which is Black/African or coloured; their ages and tenure, which are years of experience working; and their degree, which is a master's or a degree. The table below shows all these.

Code	Gender	Nationality	Race	Age	Tenure	Degree
P1	Male	South African	Black/African	45	16 years	Masters
P2	Female	South African	Black/African	44	17 years	Bachelors
P3	Female	South African	Black/African	42	14 years	Bachelors
P4	Male	South African	Black/African	48	19 years	Bachelors
P5	Male	Nigerian	Black/African	46	18 years	Masters
P6	Female	Nigerian	Black/African	50	20 years	Masters

P7	Male	South African	Black/African	45	20 years	Bachelors
P8	Male	UAE	Coloured	51	22 years	Bachelors
P9	Male	Nigerian	Black/African	50	22 years	Masters
P10	Male	South African	Black/African	54	24 years	Masters

Table 5.12: Demography profile of the respondent.

Table 5.13 below shows the Category-Code Codebook. It presents the demographic profile of respondents, including age, gender, degree, nationality, and race. The codes are female, male, degree, master, Nigerian, South African, and UAE, and each code is described.

Category-Code Codebook

Theme	Category	Code	Description
Respondent Profile	Age	-	The code represents the demographic information of participants.
	Gender	Female	The code represents the demographic information of participants.
		Male	Participant demographic information.
	Degree	Degree	Participants degree.
		Masters	Participants degree.
	Nationality	Nigerian	Participants demographic

			information.
		South African	Participants demographic information.
		UAE	Participants demographic information.
	Race	Black/African	
		Coloured	

Table 5.13: Categories-Code Codebook of the demographic profile of respondents.

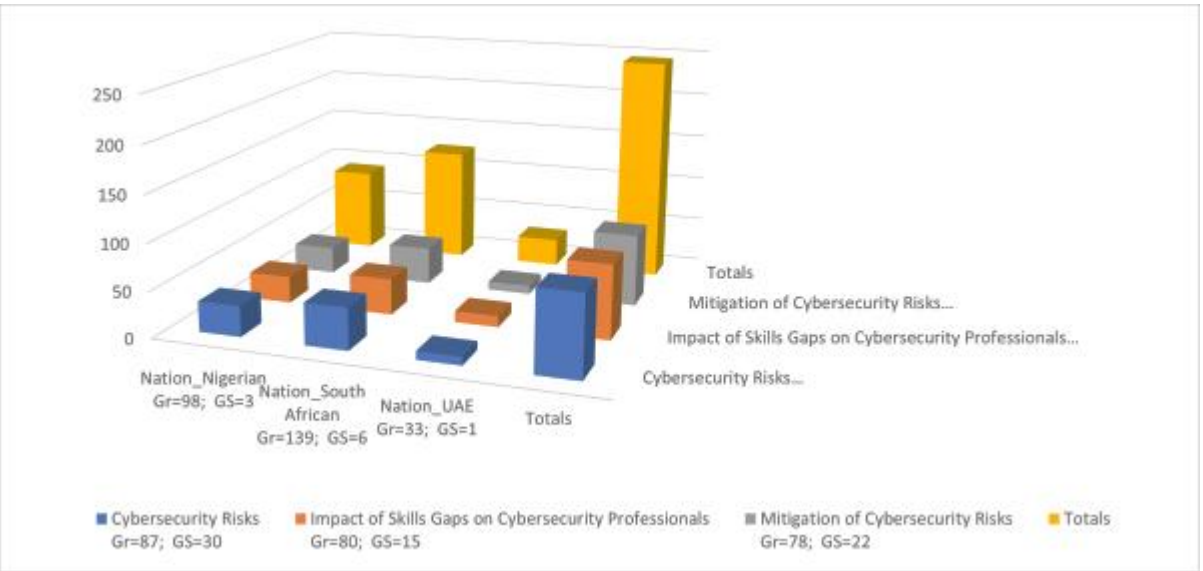


Figure 5.2: Demographics of respondents' profiles of participants' nationalities across the three themes.

Figure 5.2 above shows the bar chart graph in which Gr is the number of quotations and Gs, is the total number of categories and codes. The number of quotations for cybersecurity Risks is 87; for the mitigation of cybersecurity risks, the number of quotations is 78. There are three nationalities: Nigerian, South African, and UAE.

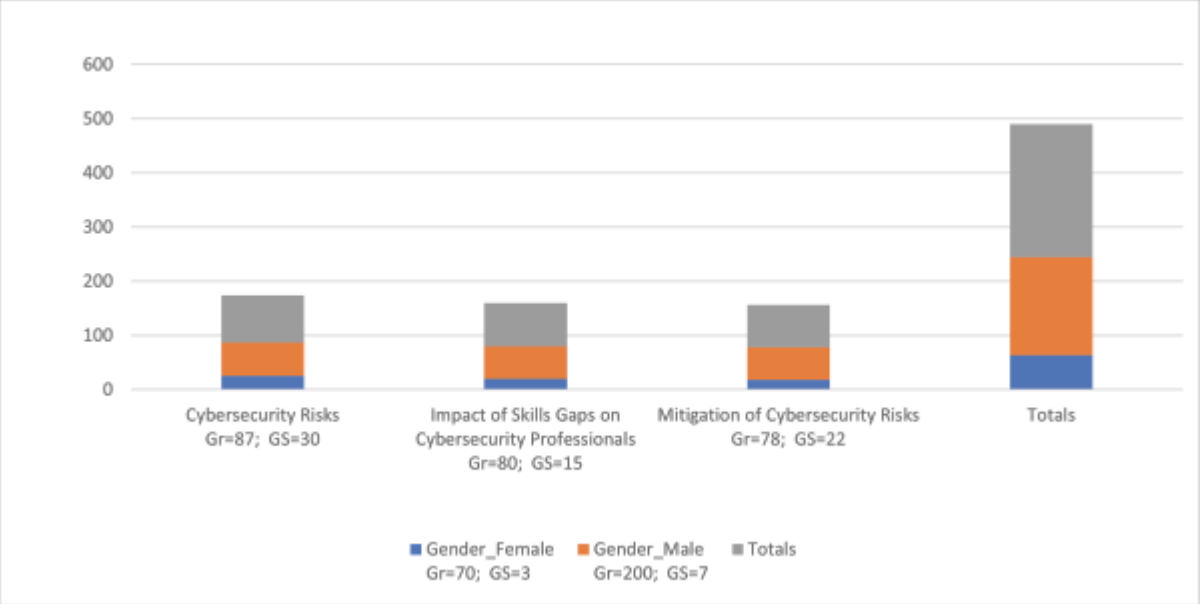


Figure 5.3: Demographics of respondent profiles on participant genders across the three themes.

From the bar chart graph above in Figure 5.3, Gr is the number of quotations, and Gs' is the total number of categories and codes. For Gender Females, the Gr is 70, and the Gs' is 3. The genders are female and male.

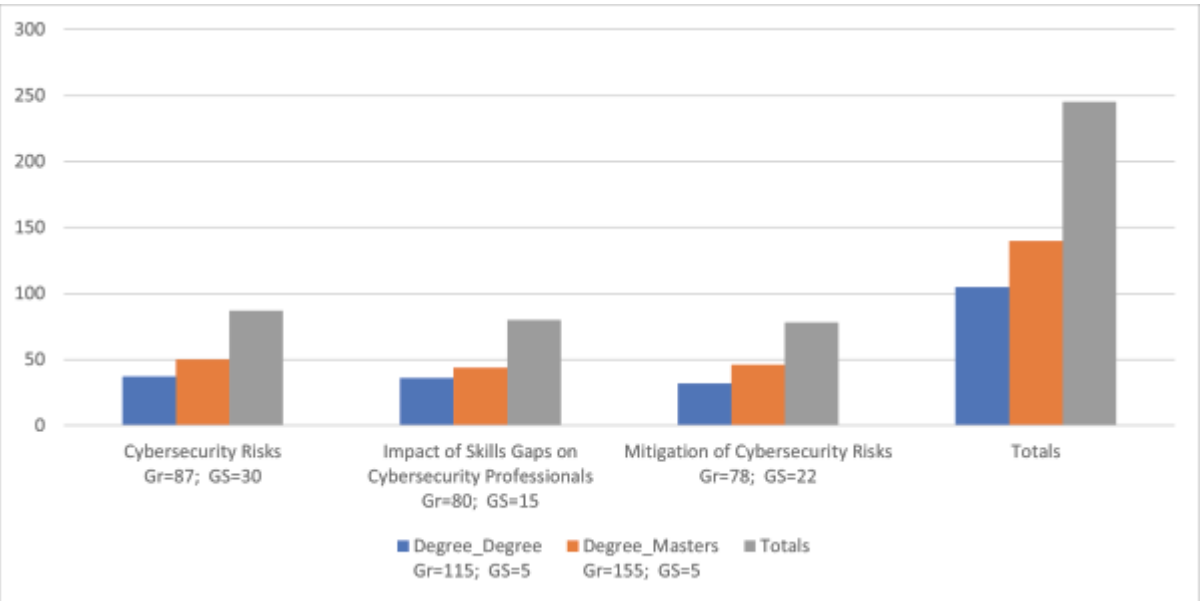


Figure 5.4: Demographics of respondents' profiles on participants' degrees across the three themes.

From the bar chart graph above in Figure 5.4, Gr is the number of quotations, while Gs' is the total number of categories and codes. The three themes are cybersecurity risks, the impacts of skills gaps on cybersecurity professionals, and the mitigation of cybersecurity risks. There are two degrees: a bachelor's and a master's.

5.3 Discussion on Proposition 1

This section discusses the similarities and differences between the findings of interview questions 1, 2, and 3, which address the first research question, and previous findings in the literature. See Table 7A in Appendix A for a comparison of theoretical expectations and findings in Proposition 1.

5.3.1 *Discussion on Interview Question 1*

The similarities and differences between the findings of interview question 1 and previous literature findings are discussed here. The similarities are as follows: Integration Points: The findings highlight vulnerabilities in integration with third-party vendors and legacy systems as critical areas. The literature suggests that similar risks are often discussed, particularly in the context of third-party risks and the need for secure integration practices (Frantti and Jallow, 2023) (see subsections 4.3.2.1.1, 4.3.2.1.5, 4.3.2.1.7, and 4.3.2.1.9). RPA and API Security: The findings emphasise the risks associated with Robotic Process Automation (RPA) and API connections, including their susceptibility to attacks due to high access levels and a potential lack of encryption. The literature indicates that these areas are frequently cited as weak points due to their role in automating critical tasks and interfacing with external systems (Afrin et al., 2024) (see subsections 4.3.2.1.2, 4.3.2.1.3, 4.3.2.1.4, and 4.3.2.1.10).

Other similarities between the findings of interview question 1 and previous findings in the literature include data privacy and Protection. According to the findings, risks associated with data in transit, data lakes, and storage systems are noted, particularly regarding sensitive customer information. The literature says that Data security is central, focusing on encryption, secure storage, and

protecting sensitive customer data (Thapa and Camtepe, 2021) (see subsections 4.3.2.1.2, 4.3.2.1.7, 4.3.2.1.8 and 4.3.2.1.10). Employee Training and Insider Threats: The findings reveal that a lack of employee awareness and the potential for insider threats pose significant vulnerabilities. Literature indicates that Employee training is a recurring need, as human error remains a leading cause of cybersecurity breaches (Ugbebor et al., 2024) (see subsections 4.3.2.1.1, 4.3.2.1.6, and 4.3.2.1.7). Incident Response and Security Frameworks: The findings underscore the necessity for robust incident response plans and comprehensive security frameworks. The literature says that Industry standards and best practices similarly emphasise these aspects as essential for mitigating risks (Knapp, 2024) (see subsection 4.3.2.1.5).

The differences between the findings of interview question 1 and previous findings in the literature are as follows: Specificity of RPA Risks: The findings provide detailed examples, such as hardcoded credentials and workflow exploitation in RPA scripts. The literature suggests that while RPA security is discussed broadly, specific risks, such as these, may not always be elaborated upon in detail (Liu et al., 2024) (see subsection 4.3.2.1.10). Focus on AI/ML Model Vulnerabilities: The findings highlight risks such as model manipulation, adversarial attacks, and compromised training data, which are uniquely outlined. The literature says that this focus on AI/ML vulnerabilities is less common, as discussions may centre more on system-level vulnerabilities (Chander et al., 2024) (see subsection 4.3.2.1.10).

Other differences between the findings of interview question 1 and previous findings in the literature are Regulatory Compliance and Reporting: The findings emphasise the need for secure compliance and regulatory reporting systems to prevent tampering. The literature suggests that compliance is a standard, but its direct link to vulnerabilities in automation technologies is not always a focal point (Fosch-Villaronga and Mahler, 2021) (see subsection 4.3.2.1.7). IoT and Endpoint Devices: Findings reveal specific vulnerabilities in IoT devices, such as ATMs and mobile payment systems. The literature says endpoint security is discussed but often in a more general sense, without focusing heavily on IoT in banking contexts (Omolara et al., 2022; Mishra, 2022) (see subsection

4.3.2.1.6). Innovative Attack Vectors: The findings discuss novel attack vectors, including tampering with AI-driven decisions and manipulating automated fraud detection systems. The literature suggests that traditional attack vectors and defences are often prioritised, with novel or emerging risks being emphasised less (Zaid and Garai, 2024) (see subsection 4.3.2.1.10). This analysis highlights the alignment and distinct contributions of the findings with existing literature, providing a comprehensive view of vulnerabilities in automated banking workflows. The new finding is that Staff training remains a critical weakness; even with advanced security, human error can lead to breaches. Banks are now focusing on continuous employee cybersecurity training to mitigate risks.

5.3.2 *Discussion on Interview Question 2*

Here is a discussion of the similarities and differences between the findings of interview question 2 and previous findings in the literature. The similarities between the findings of interview question 2 and the previous literature findings are API Security Risks: Findings highlight API vulnerabilities such as insufficient access controls, unpatched software, and insecure configurations. The literature says API security is frequently discussed in the context of automated systems due to their role in enabling integration and data exchanges (Zimmermann et al., 2022) (see subsections 4.3.2.2.6, 4.3.2.2.8, 4.3.2.2.9 and 4.3.2.2.10). Third-Party Vendor Risks: Findings emphasise risks from third-party tools, integrations, and libraries, including supply chain risks. The literature says Third-party risks are recurring, particularly when discussing the reliance on external service providers for automation technologies (George, 2024) (see subsections 4.3.2.2.2, 4.3.2.2.8, 4.3.2.2.9 and 4.3.2.2.10). RPA Risks: Findings discuss hardcoded credentials, insecure communication channels, and script tampering. The literature says similar concerns are raised about RPA tools, particularly their access to sensitive systems and potential exploitation (Asatiani et al., 2024) (see subsections 4.3.2.2.2, 4.3.2.2.5, 4.3.2.2.9 and 4.3.2.2.10).

Other similarities between the findings of interview question 2 and previous literature findings are AI and Machine Learning Vulnerabilities: Findings include adversarial attacks, data poisoning, and model theft. The literature says AI/ML-

related vulnerabilities are widely recognised, especially as these technologies become more integrated into decision-making and fraud detection systems (Abdulhussein, 2024) (see subsections 4.3.2.2.2, 4.3.2.2.5 and 4.3.2.2.10). Data Privacy and Security Risks: Findings identify data storage, transfer, and exposure risks. The literature says Data security remains a foundational concern, particularly when automation amplifies the volume and sensitivity of processed data (Klosowski, 2021) (see subsections 4.3.2.2.2, 4.3.2.2.3, 4.3.2.2.6 and 4.3.2.2.7). Insider Threats: Findings highlight risks from broad access granted to employees in automated systems. The literature says Insider threats are consistently noted as a significant risk factor due to the potential for misuse of access (Martin, 2023) (see subsection 4.3.2.2.8).

The differences between the findings in interview question 2 and previous literature findings are Cloud Security Risks: The findings highlight vulnerabilities in cloud-hosted automation platforms and data transit and storage risks. The literature says that while cloud security is discussed, it may not always be explicitly linked to automation technologies in banking (Madasamy, 2022) (see subsections 4.3.2.2.2 and 4.3.2.2.5). Phishing and Social Engineering: Findings highlight these attacks targeting automated systems and their users. The literature says such attacks are generally associated with human vulnerabilities but are less frequently tied to automation workflows (Ayiku, 2023) (see subsections 4.3.2.2.7 and 4.3.2.2.8). Legacy System Integration: Findings focus on the risks of integrating modern automation tools with outdated systems. The literature says Legacy systems are discussed broadly, but the specific challenges of transitioning during automation processes are less emphasised (Khabouze, 2022) (see subsections 4.3.2.2.6 and 4.3.2.2.10).

Other differences between the findings of interview question 2 and previous literature are Ransomware and Denial-of-Service Attacks. Findings identify these as threats to the availability and functionality of automated workflows. The literature says these attacks are common concerns but are not always explicitly tied to automation vulnerabilities (Benmalek, 2024) (see subsection 4.3.2.2.7). Supply Chain Attacks: Findings highlight risks in relying on vendors for automation tools and APIs. The literature says Supply chain risks are

discussed, but their connection to automation-specific dependencies may not always be detailed (Bacchetta et al., 2021) (see subsection 4.3.2.2.10). AI Algorithm Manipulation: Findings describe targeted attacks on AI algorithms, such as manipulating fraud detection systems. The literature says this is a relatively new and evolving area of concern, with fewer in-depth discussions than traditional vulnerabilities (Ali et al., 2024) (see subsection 4.3.2.2.6).

The findings align closely with existing literature on core cybersecurity issues, particularly API security, RPA risks, and third-party vulnerabilities. However, the findings provide a more nuanced focus on specific risks related to automation technologies, such as AI algorithm manipulation and challenges with legacy systems, which may not always be as detailed in prior literature. This distinction highlights the evolving nature of automation technologies-related cybersecurity challenges in the banking sector. A new finding not found in past literature is that AI and machine learning models are particularly vulnerable to adversarial attacks, data poisoning, and model theft, which were not previously highlighted as significant threats in past research.

5.3.3 *Discussion on Interview Question 3*

Here is the discussion of the similarities and differences between the findings of interview question 3 and previous literature findings. Here's a comparison of the findings and existing literature on how attackers exploit vulnerabilities in automated banking systems. The similarities between the findings of interview question 3 and previous literature findings are as follows: Third-Party Vendor Exploitation. The findings highlight exploitation through weak security practices in third-party systems, regulatory discrepancies, and inadequate compliance. Literature commonly discusses third-party risks, emphasising the need for rigorous vendor assessments and secure integrations (Malasowe et al., 2024) (see subsections 4.3.2.3.1 and 4.3.2.3.2). API Security Risks: Findings include API key theft, SQL injection, and cross-site scripting (XSS) attacks. The literature indicates that API vulnerabilities are frequently cited as significant attack vectors, with a focus on authentication, encryption, and input validation (Qazi, 2022) (see subsections 4.3.2.3.5 and 4.3.2.3.9). Cloud Security Risks:

Findings indicate misconfigured resources, cloud storage breaches, and unauthorised access. The literature consistently identifies cloud security as a critical concern, particularly to misconfigurations and shared responsibility models (Jonnalagadda, 2024) (see subsections 4.3.2.3.2 and 4.3.2.3.5).

Other similarities between the findings of interview question 3 and previous literature include RPA vulnerabilities. The findings discuss risks such as credential theft, workflow manipulation, and replay attacks. Literature aligns with concerns about RPA access levels and hardcoded credentials, which are often exploited by attackers (Toropov, 2025) (see subsections 4.3.2.3.2, 4.3.2.3.5, and 4.3.2.3.10). AI and Machine Learning Attacks: Findings include data poisoning, adversarial attacks, and exfiltration of models. The literature raises similar concerns about tampering with AI models, although discussions are often broader rather than focusing on specific techniques (Chander et al., 2024) (see subsections 4.3.2.3.2, 4.3.2.3.5, and 4.3.2.3.10).

The differences between the findings of interview question 3 and previous literature are Specific Exploitation Techniques for RPA. The Findings offer detailed examples, such as replay attacks and tampering with automation scripts. The literature generally discusses RPA security broadly, with less emphasis on specific attack techniques (Dhabliya et al., 2023) (see subsection 4.3.2.3.10). Focus on AI/ML Exploits: The findings provide detailed scenarios, including adversarial attacks and model exfiltration. The literature indicates that AI/ML vulnerabilities are a growing discussion area but may not always delve into as much detail regarding specific exploit methods (Abdulhussein, 2024) (see subsections 4.3.2.3.5 and 4.3.2.3.10). Operational Weakness Exploitation: Findings highlight attacks exploiting misconfigurations and operational practices, such as poorly secured devices and inadequate monitoring. Literature often focuses more on systemic vulnerabilities than operational practices (Pérez-Morón et al., 2024) (see subsection 4.3.2.3.10).

Another difference between the findings of interview question 3 and previous literature findings is the targeting of integration points. The findings address how attackers exploit integration points between automated systems and legacy frameworks. While integration risks are acknowledged, the literature says they

are not always explicitly linked to exploitation methods (Liu et al., 2022) (see subsection 4.3.2.3.9). Injection and Credential Attacks: The findings include examples such as injection attacks (SQL, malicious code) and credential stuffing. The literature suggests that broader discussions on credential-related issues may not directly tie them to automated workflows (Gestin, 2024) (see subsection 4.3.2.3.6).

The findings align with previous literature in many core areas, including third-party risks, API vulnerabilities, and the exploitation of human error. However, they provide more detailed and specific insights into modern attack strategies, such as AI/ML exploits, RPA-focused attacks, and operational weaknesses, reflecting the evolving cybersecurity landscape in automated banking. A new finding not previously reported in the literature is that attackers exploit API security risks, such as API key theft, SQL injection, and cross-site scripting (XSS), to gain unauthorised access to automated banking systems.

5.4 Discussion on Proposition 2

This section discusses the similarities and differences between the findings of interview questions 4 and 5, which address the second research question, and previous literature. See Table 8A in Appendix A for a comparison of theoretical expectations and findings in Proposition 2.

5.4.1 *Discussion on Interview Question 4*

The similarities between the findings of interview question 4 and previous literature findings are as follows: AI and Machine Learning (ML) for Threat Detection: Both the findings and previous studies highlight the use of AI and ML to monitor unusual activities in real-time, indicating a strong consensus on their effectiveness in identifying emerging threats (Walsh et al., 2024) (see subsection 4.4.2.3.6). Zero-Trust Security Model: The zero-trust architecture, which focuses on the "never trust, always verify" principle, is mentioned in both sources as a robust approach to securing systems (Alawneh and Abbadi, 2022) (see subsections 4.4.2.3.2 and 4.4.2.3.4). Multi-Factor Authentication (MFA):

MFA is consistently essential to strengthening identity and access management (Muir et al., 2024) (see subsections 4.4.2.3.2 and 4.4.2.3.6). Employee Training and Awareness: Emphasizing the human factor, the findings and previous literature stress the importance of training employees to recognise phishing, social engineering attacks, and other cybersecurity risks (Ugbebor et al., 2024) (see subsections 4.4.2.1.1 and 4.4.2.1.4).

Other similarities are evident in incident response management: developing and maintaining robust incident response plans for the timely mitigation of cybersecurity incidents is a common finding in both studies (Bitzer et al., 2023) (see subsections 4.4.2.1.3 and 4.4.2.2.2). API Security: Protecting APIs with encryption, rate limiting, and token-based authentication is a recurring recommendation (Pedro, 2024) (see subsections 4.4.2.3.2 and 4.4.2.3.5). Blockchain Technology: Blockchain is acknowledged for securing transactions and maintaining data integrity (Emiliaty, 2024) (see subsection 4.4.2.3.6). Regulatory Compliance: Both sources emphasise adhering to regulations, such as the Protection of Personal Information Act (POPIA), and international frameworks, including PCI-DSS and ISO standards (Islam, 2024) (see subsections 4.4.2.2.1 and 4.4.2.2.3).

The differences between the findings of interview question 4 and previous literature are Quantum Computing and Quantum-Resistant Cryptography: The findings introduce quantum computing defences as a proactive measure, which is not a prominent focus in earlier literature (Khatoon and Riaz, 2025). Robotic Process Automation (RPA) Security: The findings elaborate on securing RPA, including script integrity, encryption, and limiting bot privileges, which is less detailed in prior studies (Afrin et al., 2024) (see subsections 4.4.2.3.2 and 4.4.2.3.5). Collaboration with Regulators and Industry Peers: While regulatory compliance is a standard recommendation (Abikoye et al., 2024), the findings emphasise the importance of partnership with regulators and sharing intelligence with peers (see subsections 4.4.2.2.2 and 4.4.2.2.3).

Another difference is Cloud Security: The findings more prominently feature cloud computing security measures, including secure storage and access. Supply Chain Security: The findings uniquely identify securing third-party

integrations as a critical risk area, which received less attention in earlier literature (Jena et al., 2024). By synthesising these points, it becomes clear that while many foundational strategies remain consistent, the findings introduce nuanced and advanced measures, reflecting evolving cybersecurity challenges and technological advancements in the digital banking sector. A new finding not found in past literature is that banks are adopting a Zero-Trust Security Model and using AI-driven threat detection systems to monitor automated workflows, ensuring continuous real-time responses to anomalies.

5.4.2 *Discussion on Interview Question 5*

The similarities between the findings of interview question 5 and previous literature are: AI-Driven Threat Detection and Response: Both the findings and prior literature emphasise leveraging AI to detect anomalies and respond to threats in real-time, reflecting AI's growing role in cybersecurity (Anih et al., 2024) (see subsections 4.4.2.3.1 and 4.4.2.3.2). Zero-Trust Security Model: The zero-trust approach assumes no implicit trust within a network and mandates verification for all access requests, consistently acknowledged as a core strategy (Daah et al., 2024) (see subsections 4.4.2.3.2 and 4.4.2.3.5). Blockchain Technology: Using blockchain for securing transactions and ensuring data integrity is highlighted as a modern solution to cybersecurity challenges in both sources (Wenhua et al., 2023) (see subsections 4.4.2.3.1 and 4.4.2.3.5). Continuous Improvement and Adaptation: Both sources advocate for ongoing evaluation and enhancement of cybersecurity measures to address rapidly evolving threats (Zaydi, 2024).

Other similarities are Awareness and Training Programs: Employee training on cybersecurity best practices is a shared priority in mitigating human errors (Jackson and Harlee, 2024). API Security and Supply Chain Risk Management emphasise securing APIs and addressing vulnerabilities in third-party integrations to reduce risks (Das and Mukherjee, 2024) (see subsection 4.4.2.3.5). Compliance with Regulations: Adherence to regulatory frameworks (e.g., POPIA, PCI-DSS) is a shared recommendation in both findings (Lebaea et al., 2024).

The differences between the findings of interview question 5 and previous literature are: Quantum Computing and Quantum-Resistant Cryptography: The findings introduce quantum computing threats and the need for quantum-resistant cryptography, which is less emphasised in older literature (Widodo et al., 2024) (see subsection 4.4.2.3.5). Behavioural Analytics: The findings uniquely emphasise using AI for behavioural analytics to monitor user actions and detect anomalies, which has not been a prominent focus previously (Preetam, 2022) (see subsections 4.4.2.3.6 and 4.4.2.3.7). Robotic Process Automation (RPA) Security: Specific strategies to secure RPA environments, such as encrypting credentials and limiting bot privileges, are detailed in the findings but are less common in earlier findings (James, 2023) (see subsection 4.4.2.3.2).

Other differences are Dynamic and Proactive Approaches: The findings stress the need for dynamic and proactive mitigation strategies, moving beyond traditional reactive methods and highlighting the limitations of legacy systems (see subsection 4.4.2.3.10). Emergence of New Threat Vectors: Advanced threats like adversarial AI, automated exploitation of APIs, and supply chain vulnerabilities are given specific attention in the findings (see subsection 4.4.2.3.10). Collaboration and Intelligence Sharing: Collaboration is a standard recommendation (Troussas et al., 2023), but the findings emphasise intelligence sharing within the financial sector and with regulators. This comparison demonstrates that while foundational strategies are consistent, the research findings reflect advancements in technologies and methodologies, highlighting the need for innovation to address emerging risks in the digital banking landscape. This study's new finding is that traditional cybersecurity strategies are insufficient; quantum-resistant cryptography and blockchain-based validation are now being explored to secure automation technologies.

5.5 Discussion on Proposition 3

This section discusses the similarities and differences between the findings of interview questions 6, 7, and 8 of the third research question and previous

literature findings. See Table 9A in Appendix A for a comparison of theoretical expectations and findings in Proposition 3.

5.5.1 *Discussion on Interview Question 6*

The similarities between the findings of interview question 6 and those in the previous literature are discussed here. AI and Machine Learning (AI/ML) Skills: Both the findings and previous literature emphasise the importance of AI/ML expertise, particularly in securing AI models, detecting adversarial attacks, and mitigating data poisoning risks (Markonda and Pannala, 2023) (see subsections 4.5.2.1.2, 4.5.2.1.5 and 4.5.2.1.10). These skills align with the growing reliance on AI for decision-making in digital banking (Prakash et al., 2023). Cloud Security Skills: Cloud security is highlighted in both contexts, focusing on securing cloud-based infrastructure, managing multi-cloud environments, and ensuring compliance with cloud security standards (Seth et al., 2024) (see subsections 4.5.2.1.2, 4.5.2.1.5 and 4.5.2.1.9). Data Privacy and Protection: The findings and prior research emphasise the importance of expertise in data lifecycle management, privacy compliance, and the protection of sensitive data, reflecting global concerns about data breaches and regulatory compliance (Sargiotis, 2024) (see subsections 4.5.2.1.2 and 4.5.2.1.7).

Other similarities between the findings of interview question 6 and previous literature findings are as follows: DevSecOps: Incorporating security into the development lifecycle (DevSecOps) recurred, emphasising continuous integration, delivery, and secure software development (Adewole, 2024) (see subsection 4.5.2.1.5). Identity and Access Management (IAM): Both emphasise IAM as a critical skill to manage access across complex, automated systems effectively (Rawal et al., 2023) (see subsections 4.5.2.1.2 and 4.5.2.1.5). API Security: Securing APIs is vital, as evidenced by findings and previous literature, given the growing role of APIs in enabling digital banking automation technologies (Domoney, 2024) (see subsection 4.5.2.1.5). Foundational Cybersecurity Skills: Traditional skills, such as network security, penetration testing, and incident response, are acknowledged as essential in both sets of

findings but need to be expanded to incorporate emerging automation technologies (Owusu, 2023) (see subsection 4.5.2.1.8).

The differences between the findings of interview question 6 and previous literature findings are as follows: RPA Security: The findings uniquely emphasise securing robotic process automation (RPA) workflows, a specialisation less emphasised in traditional cybersecurity literature (Eulerich et al., 2024) (see subsections 4.5.2.1.8 and 4.5.2.1.10). Quantum Computing-Resistant Cryptography: The findings highlight this skill set, which is not a common feature of earlier discussions, reflecting a more forward-looking perspective on emerging threats (Easttom, 2022) (see subsection 4.5.2.1.5).

Other differences between the findings of interview question 6 and previous literature findings are as follows: Shift from Reactive to Proactive Approaches: The findings emphasise a proactive approach using AI tools to anticipate attacks, contrasting with the more reactive stance described in older frameworks (Ajala et al., 2024) (see subsection 4.5.2.1.8). Integration of Emerging Technologies: The findings explicitly highlight skills in blockchain, IoT, and programming languages such as Python and Java, reflecting a broader integration of IT and OT security (see subsections 4.5.2.1.5 and 4.5.2.1.6). Soft Skills: The findings emphasise non-technical skills, such as communication, collaboration, and adaptability, to navigate complex regulatory environments and drive innovation in digital banking security (see subsection 4.5.2.1.5).

This analysis highlights how the findings build upon established literature while incorporating new dimensions to address the evolving cybersecurity landscape in the context of digital banking automation technologies in South Africa. The latest finding of this study is that AI security expertise, adversarial attack defence, and API security management have emerged as critical skills, shifting the focus beyond traditional network security.

5.5.2 *Discussion on Interview Question 7*

The similarities between the findings of interview question 7 and previous literature findings are as follows: Collaboration with Educational Institutions:

Both the findings and previous literature emphasise forming partnerships with universities, colleges, and technical schools to develop curricula tailored to industry needs. This includes internships, apprenticeships, and hands-on training programs (Kebede et al., 2024) (see subsections 4.5.2.2.1 and 4.5.2.2.10). Investment in Training and Upskilling: The findings and literature widely recognise the need for targeted training programs and the upskilling of existing staff using certifications, workshops, and online platforms (e.g., Coursera, Udemy) (Chakraborty and Tripathi, 2024) (see subsections 4.5.2.2.2, 4.5.2.2.4, 4.5.2.2.6, 4.5.2.2.7, 4.5.2.2.8, 4.5.2.2.9 and 4.5.2.2.10).

Other similarities between the findings of interview question 7 and previous literature are as follows: Public-Private Partnerships. Previous studies and findings highlight the importance of government and industry collaboration in funding and scaling education and training initiatives (Leal Filho et al., 2024) (see subsection 4.5.2.2.5). Technology Integration in Training: Both sources support integrating advanced automation technologies and digital banking tools into training programs to provide hands-on experience (Familoni and Onyebuchi, 2024) (see subsection 4.5.2.2.7). Focus on STEM and Digital Literacy: Promoting STEM education and grassroots digital literacy programs aligns with the recommendations in the literature and the findings (Miller, 2024) (see subsection 4.5.2.2.5).

The differences between the findings of interview question 7 and previous literature findings are Specificity in Certifications: The findings emphasise micro-certifications and targeted certifications in areas like RPA (Robotic Process Automation), AI governance, and API management, which are less elaborated in earlier literature (Nwankwo et al., 2022) (see subsections 4.5.2.2.5, 4.5.2.2.6 and 4.5.2.2.9). Tailored Solutions for South Africa: The findings highlight South Africa-specific strategies, including addressing local cybersecurity challenges and leveraging government policies to create incentives. Previous literature often addresses broader, global strategies without tailoring them to the South African context (Parry et al., 2024) (see subsection 4.5.2.2.8). Focus on Attracting Talent: The findings uniquely emphasise attracting new talent through partnerships with tech hubs and competitive benefits, such as flexible work

arrangements and diversity initiatives, which is not often a primary focus in the broader literature (Van Hoa and Van Thu, 2024) (see subsection 4.5.2.2.6).

Other differences between the findings of interview question 7 and previous literature findings are Grassroots Initiatives: While grassroots digital literacy is mentioned, the findings place a stronger emphasis on community-level programs and starting skills development at schools, which are not as emphasised in previous studies (Moser and Bader, 2023) (see subsection 4.5.2.2.8). Integration of Automation Technologies-Specific Skills: The findings suggest that automation technologies, such as RPA and AI, should be integrated into existing academic programs, which may not always be highlighted in prior literature (Babashahi et al., 2024) (see subsections 4.5.2.2.7 and 4.5.2.2.10). These comparisons highlight how the findings align with and expand upon existing knowledge, particularly by tailoring solutions to the South African digital banking context. A new finding is that banks increasingly collaborate with universities and tech firms to develop targeted cybersecurity training programs that align with real-world digital banking threats.

5.5.3 *Discussion on Interview Question 8*

The similarities between the findings of interview question 8 and previous literature are as follows: Balanced Approach. The findings and previous literature advocate for a hybrid strategy that combines retraining existing professionals and attracting new talent. This ensures a workforce capable of adapting to immediate and long-term challenges (Bari and Di Virgilio, 2025) (see subsections 4.5.2.2.5, 4.5.2.2.7, 4.5.2.2.8 and 4.5.2.2.9). Value of Existing Professionals: Both sources agree on leveraging the institutional knowledge and experience of current employees. Retraining existing staff is highlighted as cost-effective and beneficial for retaining organisational culture and expertise (Spielman et al., 2024) (see subsection 4.5.2.2.1). Necessity of New Talent: The findings and previous literature emphasise the need to attract new talent with specialised skills, particularly in emerging areas such as AI, machine learning, and cybersecurity. Fresh talent brings innovative ideas and diverse

perspectives to drive organisational growth and innovation (Chew and Mohamed Zainal, 2024) (see subsection 4.5.2.2.1).

Another similarity is Long-Term Sustainability: Both sources emphasise the importance of establishing a sustainable pipeline of skilled professionals through partnerships with educational institutions and structured mentorship programs (Teodorescu et al., 2024) (see subsection 4.5.2.2.10). Immediate and Strategic Needs: The dual focus on addressing immediate skill gaps with retraining and preparing for future demands by hiring specialists aligns with prior research (Li, 2022) (see subsection 4.5.2.2.10).

The differences between the findings of interview question 8 and previous literature are as follows: Emphasis on Retention. The findings emphasise the benefits of employee retention and morale through retraining, highlighting it as a method to reduce turnover and maintain continuity. Previous literature may not have explored retention as profoundly as this study (Padma, 2024) (see subsection 4.5.2.2.10). Proportional Approach: The findings suggest a practical division of effort, with a focus of 60-70% on retraining and 30-40% on attracting new talent. This quantitative breakdown is less commonly discussed in broader literature (see subsection 4.5.2.2.5).

Another difference between the findings of interview question 8 and previous literature is the inclusion of practical examples. The findings highlight case studies and examples, such as the implementation of AI-driven fraud detection systems with retrained staff. Such detailed, real-world applications might not always be found in traditional literature (see subsection 4.5.2.2.6). These comparisons highlight that while the findings align with existing research, they provide additional regional context, practical strategies, and a more explicit focus on retention and mentoring. A New Finding is that a hybrid approach is preferred—existing professionals undergo retraining in AI and automation security. At the same time, new talent is brought in for specialised cybersecurity skills that current staff may lack.

5.6 Conclusion

Proposition 1: "New cybersecurity threats will emerge as automation technologies transform the Future of Work in digital banking." The discussions confirm this proposition. Key findings align with the existing literature on emerging cybersecurity threats associated with automation technologies, including RPA, APIs, and AI/ML. Specific vulnerabilities identified include integration points, which pose risks when integrating legacy systems with modern automated tools. AI/ML Exploits: The manipulation of AI models and the use of adversarial attacks are becoming increasingly prominent. RPA Risks: Detailed risks, such as hardcoded credentials and workflow exploitation, were uniquely outlined. Novel Attack Vectors: AI-driven decision tampering and automated fraud detection manipulation were highlighted, showing emerging risks beyond traditional concerns. These findings reinforce the inevitability of new cybersecurity challenges as automation technologies advance, emphasising the need for adaptive and proactive strategies. New Finding: While previous research highlighted API security and insider threats, this study reveals that adversarial attacks on AI models and data poisoning are emerging as significant risks. Attackers can manipulate AI-driven banking processes, bypassing fraud detection systems in unprecedented ways.

Proposition 2: "South Africa's digital banking sector can leverage automation technologies to enhance operational efficiency and proactively mitigate cybersecurity threats from its growing reliance on automated systems." This proposition is supported by discussions that highlight both opportunities and challenges. Key points include AI for Threat Detection: Real-time monitoring and anomaly detection using AI/ML were widely noted as practical measures. Zero-Trust Security Models: Adopting “never trust, always verify” principles aligns with securing automated systems. Collaboration and Compliance: Regulatory adherence and collaboration with peers and regulators are foundational strategies. Advanced Measures: Proactive measures such as quantum-resistant cryptography, dynamic authentication, and continuous improvement reflect evolving cybersecurity practices. While operational efficiencies are evident, the findings stress the importance of adopting

advanced and region-specific strategies to mitigate risks effectively. New Finding: Unlike past literature, which primarily emphasised compliance-based security approaches, this study identifies the growing importance of AI-powered security, blockchain-based transaction validation, and the Zero-Trust Security Model as proactive strategies to mitigate automation technologies-related cybersecurity risks.

Proposition 3: "The fast-growing use of digital banking automation technologies will affect the cybersecurity skills gap in South Africa's future workforce." This proposition is validated, with discussions revealing significant implications for the cybersecurity skills landscape. Key findings include New Skill Requirements: AI/ML expertise, RPA security, and quantum-resistant cryptography are emerging as critical areas for skill development. Shift in Training Approaches: Focus on integrating automation technologies into existing training programs and adopting a proactive stance toward skill enhancement. Localised and Tailored Strategies: Emphasis on addressing South Africa-specific challenges through grassroots initiatives, partnerships with educational institutions, and leveraging public-private collaborations. Workforce Retention and Development: Balancing retraining existing professionals and attracting new talent is highlighted as a sustainable approach, with structured mentorship and practical training programs playing a central role. These findings underline the need for a balanced and forward-looking strategy to address the cybersecurity skills gap in the face of growing automation. New Finding: While previous studies acknowledged the skills gap, this research highlights that South African banks are shifting towards a hybrid approach—retraining existing professionals in AI security and DevSecOps while actively recruiting new talent with expertise in machine learning security, API protection, and cloud security.

The discussions support all three propositions, highlighting the transformative impact of automation technologies on cybersecurity threats, operational efficiencies, and workforce skills in South Africa's digital banking sector. The findings emphasise proactive measures, regional customisation, and a focus on evolving technologies to mitigate risks and harness opportunities effectively.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter presents conclusions regarding Research Questions 1, 2, and 3, as well as recommendations for each stakeholder and suggestions for further research. This study uncovered the following in cybersecurity: Major Cybersecurity Threats Identified. The research revealed several critical threats resulting from the integration of automation technologies into digital banking systems. These threats include phishing and social engineering, where attackers increasingly use deceptive tactics to trick staff or customers into disclosing sensitive information. Malware and Ransomware: Automated systems are frequently targeted by malicious software, which can sometimes result in a total system lockdown or ransom demands. Insider Threats: Employees or contractors with legitimate access may pose intentional or unintentional threats to cybersecurity. Password and Credential Attacks: Weak or reused credentials are vulnerable to brute-force or dictionary attacks. Distributed Denial of Service (DDoS) Attacks: Overwhelming banking systems with traffic, causing service disruptions. These threats are exacerbated by automation's ability to scale processes quickly, both positively and negatively.

Automation technologies increase the Cyber Attack Surface. The study found that increased reliance on interconnected, automated systems (e.g., chatbots, RPA, AI monitoring tools) creates more entry points for cybercriminals. Complex systems mean more vulnerabilities, especially where legacy systems have not been updated. Cybersecurity Skills Gap: A critical shortage of skilled cybersecurity professionals exists, rendering them unable to effectively manage the risks introduced by automation technologies. The study identified that many banks lack in-house expertise and rely on general IT staff without deep security training. The demand for upskilling is high, and organisations must invest in continuous learning to build internal capabilities. Mitigation Strategies Are Inconsistent and Reactive: Some banks utilise advanced mitigation tools, such as AI monitoring, SIEM, or digital identity systems. However, approaches are

often reactive rather than proactive, with poor integration of training, awareness, and governance policies.

The study recommended the use of cybersecurity frameworks (e.g., NIST RMF, ISO 27005) and the need for more decisive leadership in their implementation. Regulatory Challenges Exist: The study revealed that existing cybersecurity regulations in South Africa struggle to keep pace with the evolving risks of automation technologies. Regulators are perceived as slow to adapt, and there is a lack of unified enforcement or industry-wide standards. Human Factors Are Underestimated: Many vulnerabilities arise from human error, lack of awareness, and organisational resistance to cybersecurity protocols. Despite this, most mitigation efforts are technology-focused, with insufficient investment in behavioural and cultural change. Importance of Governance and Leadership: The study found that organisations with strong leadership and governance structures are more prepared for cyber threats. Leaders who promote a culture of security awareness and provide ongoing staff training contribute significantly to reduced risk exposure.

In summary, the study offers a detailed, practical, and context-specific understanding of cybersecurity in South Africa's digital banking sector. It demonstrates that automation technologies introduce both new opportunities and new vulnerabilities, and that effective mitigation depends not only on tools and technologies, but also on people, policies, and leadership.

6.2 Conclusions Regarding Research Question 1

Research Question 1: "What are the cybersecurity threats posed by automation technologies of the future of work in digital banking?" While enhancing operational efficiency, the study identified that automation technologies also introduce significant cybersecurity vulnerabilities. Key threats include API security risks, such as API key theft, SQL injection, and cross-site scripting (XSS). AI and Machine Learning Exploits: Adversarial attacks, data poisoning, and model theft. RPA Vulnerabilities: Credential theft, process manipulation, and workflow exploitation. Integration and Third-Party Risks: Issues arising from

third-party environments, insufficient integration safeguards, and legacy system vulnerabilities. Human Factors: A lack of staff training was highlighted as a recurring factor that exacerbates cybersecurity risks. Conclusion: Automation technologies necessitate proactive and robust security strategies to address emerging threats.

6.3 Conclusions Regarding Research Question 2

Research Question 2: "How can the South African digital banking industry mitigate the cybersecurity risks identified from bringing on board automation technologies for the future of work in the banking sector?" Mitigation strategies include Organisational Measures: Regular employee training, robust incident response planning, and continuous security audits. Technological Solutions: Adoption of advanced technologies, including AI-powered threat detection, zero-trust architecture, blockchain for transaction integrity, and multi-factor authentication. Regulatory Compliance: Collaboration with regulatory bodies, adherence to local and international standards (e.g., POPIA, PCI-DSS), and regular compliance audits. Conclusion: By leveraging cutting-edge automation technologies, fostering regulatory compliance, and implementing robust organisational measures, South African banks can proactively address cybersecurity threats while improving efficiency.

6.4 Conclusions Regarding Research Question 3

Research Question 3: "How does identifying cybersecurity risks associated with digital banking automation technologies in the future of work in South Africa impact the skills gap in cybersecurity professionals?" Key findings regarding the impact of the skills gap include the following: Emerging Skills Needs - Expertise in securing AI models, RPA workflows, cloud infrastructure, and API security is critical. New competencies in automation technologies must complement traditional cybersecurity skills. Bridging the Skills Gap: Strategies include targeted training programs, partnerships with educational institutions, and leveraging online learning platforms. A balanced approach to retraining existing professionals, while also attracting new talent, is recommended. Long-Term

Educational Initiatives: Developing curricula aligned with industry needs and promoting STEM education and cybersecurity awareness at earlier stages. Conclusion: The rapid adoption of automation technologies creates a pressing need for new skill sets, necessitating both the retraining of current professionals and the recruitment of new talent to address the evolving cybersecurity landscape.

6.5 Recommendations

Based on this study's discoveries, recommendations to each stakeholder are as follows:

Employees: Training and Awareness: Regular, practical training sessions to develop skills in identifying and mitigating cybersecurity threats, including phishing and social engineering. Upskilling Initiatives: Invest in certifications and programs focused on emerging cybersecurity fields, such as API security, AI/ML security, and cloud security. Encourage a Learning Culture: Foster an environment that supports continuous education on advanced automation technologies and cybersecurity trends.

Customers: Awareness Campaigns: Educate customers on cybersecurity practices, such as recognising phishing attempts and using multi-factor authentication. Enhanced Security Features: Implement robust biometric authentication and educate users about its benefits to encourage adoption. User-Friendly Security Updates: Ensure that updates and security features are designed with accessibility and usability in mind.

Suppliers: Vendor Risk Management: Enforce strict compliance with cybersecurity standards for third-party vendors. Secure Integrations: Employ secure API and data-sharing protocols to minimise vulnerabilities in connected systems. Continuous Audits: Conduct regular security assessments for suppliers and partners.

Investors: Highlight Cybersecurity Initiatives - Communicate the organisation's commitment to robust cybersecurity measures as part of its risk management

strategy. Transparency in Reporting: Share information on mitigation strategies and successes in preventing cyber incidents. Strategic Investments: Advocate for funding technologies such as AI-driven threat detection and blockchain to enhance cybersecurity.

Competitors: Collaborative Cybersecurity Forums: Encourage industry-wide cooperation to share intelligence on emerging threats and best practices. Standardisation Efforts: Work with competitors to establish common frameworks for cybersecurity in digital banking. Avoid Adversarial Exploitation: Emphasise ethical competitiveness, avoiding tactics that exploit cybersecurity vulnerabilities.

Government: Policy Development: Create regulations mandating robust cybersecurity measures for banking automation technologies. Public-Private Partnerships: Foster collaboration with banks and educational institutions to address the cybersecurity skills gap. Incentives for Compliance: Offer tax incentives or grants to organisations that invest in advanced cybersecurity systems.

6.6 Contributions

The contributions of this study include:

- **Academic Advancement**. The study contributes valuable insights to the body of knowledge, particularly in the context of cybersecurity risks associated with automation technologies in South Africa's digital banking sector. It also enhances the researcher's qualifications and provides insights for future researchers who may build on its findings.

- **Practical Impact on Digital Banking**. Beyond its academic contributions, the research seeks to offer practical solutions to the cybersecurity challenges faced by digital banking institutions in South Africa. These solutions may help enhance financial asset protection, prevent fraud, improve data privacy, and increase customer trust.

- **Technological Innovation and Economic Stability**. By identifying cybersecurity threats and developing mitigation strategies, the study promotes technological innovation and contributes to a more stable economic environment in the banking sector.

- **Professional Development and Industry Applications**. The study examines the impact of automation technologies on the cybersecurity skills gap, providing recommendations for upskilling employees, developing training programs, and enhancing workforce readiness in the banking sector.

- **Policy and Regulatory Contributions**. The insights from this study can help policymakers and regulators enhance cybersecurity frameworks, compliance measures, and risk management practices in the banking industry.

This research makes a significant contribution to academia and industry, enabling digital banking institutions to navigate cybersecurity challenges while leveraging automation technologies for a secure and innovative future.

6.7 Suggestions for further research

Based on the literature search and research conducted, suggestions for further investigation include Cybersecurity Education Programs: Examine the effectiveness of current training methods and explore new models tailored to digital banking automation technologies. Emerging Threats: Examine the evolving nature of threats, such as adversarial AI attacks and supply chain vulnerabilities, in the banking sector. Economic Impact: Assess the financial implications of cybersecurity breaches and the cost-effectiveness of mitigation strategies. Automation Technology Adoption: Analyse the potential of advanced automation technologies, such as blockchain and quantum-resistant cryptography, to address cybersecurity challenges. Cross-Industry Insights: Compare cybersecurity practices across industries to identify transferable strategies for digital banking. Behavioural Studies: Examine user and employee

behaviour to develop targeted interventions for reducing human error in cybersecurity practices.

REFERENCES

1. Abdulhamid, A., Kabir, S., Ghafir, I., & Lei, C. (2022, November). Dependability of the internet of things: Current status and challenges. In *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)* (pp. 1-6). IEEE.

2. Abdulhussein, M. (2024). *The impact of artificial intelligence and machine learning on organizations cybersecurity*. Liberty University.

3. Abikoye, B. E., Umeorah, S. C., Adelaja, A. O., Ayodele, O., & Ogunsuji, Y. M. (2024). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. *World Journal of Advanced Research and Reviews*, *23*(1), 18301844.

4. Abulencia, J. (2021). Insider attacks: Human-factors attacks and mitigation. *Computer Fraud & Security*, *2021*(5), 14-17.

5. Acharya, R. (2024). Examining Interpretivism in Social Science Research. *Education*.

6. Achor, O. (2023). *Data Security Strategies for Preventing Breaches Due to Insider Threats* (Doctoral dissertation, Walden University).

7. Adebayo, A., & Ackers, B. (2021). Sampling theoretically for comparison. *Electronic Journal of Business Research Methods*, *19*(1), pp42-56.

8. Adeleye, R. A., Asuzu, O. F., Bello, B. G., Oyeyemi, O. P., & Awonuga, K. F. (2024). Digital currency adoption in Africa: A critical review and global comparison. *World Journal of Advanced Research and Reviews*, *21*(2), 130-139.

9. Adeoye, M. A. (2023). Review of sampling techniques for education. *ASEAN Journal for Science Education*, *2*(2), 87-94.

10. Adewole, S. A. (2024). Navigating the Complexities of DevSecOps: A Comprehnsive Exploration of Organizational, Cultural & SocioTechnical Factors.

11. Adjasi, C. K., & Yu, D. (2021). Investigating South Africa's economic growth: The role of financial sector development. *Journal of Business and Economic Options*, *4*(3), 19-29.

12. Afrin, S., Roksana, S., & Akram, R. (2024). AI-Enhanced Robotic Process Automation: A Review of Intelligent Automation Innovations. *IEEE Access*.

13. Aguinis, H. (2023). *Research methodology: Best practices for rigorous, credible, and impactful research*. SAGE Publications.

14. Ahmed, F., Hussain, A., Khan, S. N., Malik, A. H., Asim, M., Ahmad, S., & El-Affendi, M. (2024). Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers.

15. Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *2*, 100051.

16. Ahvanooey, M. T., Zhu, M. X., Li, Q., Mazurczyk, W., Choo, K. K. R., Gupta, B. B., & Conti, M. (2021). Modern authentication schemes in smartphones and IoT devices: An empirical survey. *IEEE Internet of Things Journal*, *9*(10), 7639-7663.

17. Aithal, P. S. (2023). Enhancing Industrial Automation through Efficient Technology Management in Society. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *7*(4), 184-215.

18. Ajala, O. A., Okoye, C. C., Ofodile, O. C., Arinze, C. A., & Daraojimba, O. D. (2024). Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time. *Magna Scientia Advanced Research and Reviews*, *10*(1), 312-320.

19. Ajayi, F. A., & Udeh, C. A. (2024). Review of workforce upskilling initiatives for emerging technologies in IT. *International Journal of Management & Entrepreneurship Research*, *6*(4), 1119-1137.

20. Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud Security Challenges and Solutions: A Review of Current Best Practices.

21. Al-Ahmad, W., & Mohammad, B. (2013). Addressing information security risks by adopting standards. *International Journal of Information Security Science*, *2*(2), 28-43.

22. Alahmadi, B. A., Axon, L., & Martinovic, I. (2022). 99% false positives: A qualitative study of {SOC} analysts' perspectives on security alarms. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 2783-2800).

23. Alawneh, M., & Abbadi, I. M. (2022, November). Integrating trusted computing mechanisms with trust models to achieve zero trust principles. In *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 1-6). IEEE.

24. AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

25. Alhawamdeh, A. K., Mohammad, A. M., Alshaketheep, K., Padlee, S. F., & Al-Shamaileh, I. (2024). Fostering Customer Satisfaction and Loyalty in Jordanian Banks: A Digital Approach Through Philanthropic and Environmental Responsibility. *International Journal of Sustainable Development & Planning*, *19*(1).

26. AL-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *momentum*, *3*(14), 15.

27. Alhazmi, A. A., & Kaufmann, A. (2022). Phenomenological qualitative methods applied to the analysis of cross-cultural experience in novel educational social contexts. *Frontiers in Psychology*, *13*, 785134.

28. Alheadary, W. G. (2023). Towards Development of a Security Risk Assessment Model for Saudi Arabian Business Environment Based on the ISO/IEC 27005 ISRM Standard. *Journal of Information Security*, *14*(3), 195-211.

29. Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M., & Adamopoulos, I. (2024). A survey on artificial intelligence in cybersecurity for smart agriculture: state-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. *Mesopotamian Journal of Computer Science*, *2024*, 53-103.

30. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

31. Al-Mudaires, F., Al-Samawi, A., Aljughaiman, A., & Nissirat, L. (2023). Information security risk management framework for a governmental educational institute. *Journal of Information and Knowledge Management (JIKM)*, *13*(1), 36-54.

32. AlSadhan, T. (2022). *Leveraging Information Security Continuous Monitoring (ISCM) to Enhance Cybersecurity* (Doctoral dissertation, Syracuse University).

33. Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, *11*(20), 3330.

34. Amat-Lefort, N., & Barnes, S. J. (2024). An Inconvenient Truth: Understanding Service Inconvenience in Digital Platforms. *Journal of Service Research*, 10946705241254735.

35. Amin, M. E. K., Nørgaard, L. S., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A., & Desselle, S. P. (2020). Establishing trustworthiness and authenticity in qualitative pharmacy research. *Research in social and administrative pharmacy*, *16*(10), 1472-1482.

36. Anshari, M., Almunawar, M. N., Lim, S. A., & Al-Mudimigh, A. (2019). Customer relationship management and big data enabled: Personalization & customization of services. *Applied Computing and Informatics*, *15*(2), 94-101.

37. Arnaut, D., & Bećirović, D. (2023). FinTech innovations as disruptor of the traditional financial industry. In *Digital Transformation of the Financial Industry: Approaches and Applications* (pp. 233-254). Cham: Springer International Publishing.

38. Arora, N., & Gupta, S. (2020). Total quality management for employee engagement: a study. *Test Engineering and Management*, *82*, 12769-86.

39. Asatiani, A., Hakkarainen, T., Paaso, K., & Penttinen, E. (2024). Security by envelopment–a novel approach to data-security-oriented configuration of lightweight-automation systems. *European Journal of Information Systems*, *33*(5), 631-653.

40. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

41. Axon, L., Fletcher, K., Scott, A. S., Stolz, M., Hannigan, R., Kaafarani, A. E., ... & Creese, S. (2022). Emerging cybersecurity capability gaps in the industrial internet of things: Overview and research agenda. *Digital Threats: Research and Practice*, *3*(4), 1-27.

42. Atatsi, E. K. (2024). *Exploring the Use of Internships to Build Practical Experience for Emerging Cybersecurity Professionals in Order to Meet Industry Work Experience Requirements* (Doctoral dissertation, Marymount University).

43. Ayiku, D. (2023). *Comparative Analysis: The increase in phishing activities* (Doctoral dissertation, Aalborg University).

44. Babashahi, L., Barbosa, C. E., Lima, Y., Lyra, A., Salazar, H., Argôlo, M., ... & Souza, J. M. D. (2024). AI in the Workplace: A Systematic Review of Skill Transformation in the Industry. *Administrative Sciences*, *14*(6), 127.

45. Bacchetta, M., Bekkers, E., Piermartini, R., Rubinova, S., Stolzenburg, V., & Xu, A. (2021). COVID-19 and global value chains. *World Trade Organisation*.

46. Bahia, T. H. A., Abbas, B. A. H., & Idan, A. R. (2023). Total quality management as a philosophy to improve the performance of the academic organization. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(1), 19.

47. Ban, T., Takahashi, T., Ndichu, S., & Inoue, D. (2023). Breaking alert fatigue: Ai-assisted siem framework for effective incident response. *Applied Sciences*, *13*(11), 6610.

48. Barath, M., & Schmidt, D. A. (2022). Offices after the COVID-19 pandemic and changes in perception of flexible office space. *Sustainability*, *14*(18), 11158.

49. Bari, M. W., & Di Virgilio, F. (Eds.). (2025). *Handbook of Talent Management and Learning Organizations: A Post-Pandemic Perspective*. CRC Press.

50. Barnard, D., & Moolman, J. www. sangonet. org. za. *Global Information Society Watch 2008*, 175.

51. Baseri, Y., Chouhan, V., & Ghorbani, A. (2024). Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure. *arXiv preprint arXiv:2404.10659*.

52. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*, 139-154.

53. Baskerville, R., Capriglione, F., & Casalino, N. (2020). Impacts, challenges and trends of digital transformation in the banking sector. *Law and Economics Yearly Review Journal-LEYR, Queen Mary University, London, UK*, *9*(part 2), 341-362.

54. Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), 359-374.

55. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849-3886.

56. Bello, O. A. (2024). The role of data analytics in enhancing financial inclusion in emerging economies. *International Journal of Developing and Emerging Economies*, *11*(3), 90-112.

57. Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*.

58. Bethlehem, J. (2021). Challenges of Online Non-Probability Surveys. In *Handbook of Computational Social Science, Volume 2* (pp. 181-195). Routledge.

59. Bindseil, U., & Pantelopoulos, G. (2022). Towards the holy grail of cross-border payments.

60. Bingle, Y. G. (2022). *Your Cyber Technical Skills Will get You Hired, but Your Lack of Soft Skills can get You Fired* (Doctoral dissertation, Marymount University).

61. Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, *15*(02), 245-278.

62. Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable–A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050.

63. Björnsdottir, S. H., Jensson, P., Thorsteinsson, S. E., Dokas, I. M., & de Boer, R. J. (2022). Benchmarking ISO risk management systems to assess efficacy and help identify hidden organizational risk. *Sustainability*, *14*(9), 4937.

64. Borg, F., & Persson, M. (2010). Assessing Factors Influencing the Diffusion of Mobile Banking in South Africa-A case study on the company Wizzit.

65. Borgia, M. S., Di Virgilio, F., La Torre, M., & Khan, M. A. (2022). Relationship between work-life balance and job performance moderated by knowledge risks: are bank employees ready?. *Sustainability*, *14*(9), 5416.

66. Bronson, H. E. (2022). *Five Common Shortcomings of Third-Party Management Programs in Financial Organizations and Recommended Risk Management Strategies* (Master's thesis, Utica University).

67. Brotherston, L., Berlin, A., & Reyor III, W. F. (2024). *Defensive security handbook*. " O'Reilly Media, Inc.".

68. Busch, D. (2024). The Knock-On Effect of Financial Supervision Law in Civil Liability Law. *Journal of European Tort Law*, *15*(3), 225-263.

69. Caffer, P., Brisolara, S., Hernández, A. E., & Jefferson, A. (2024). Ethnographic Inquiry in Program Evaluation: Ensuring Authenticity and Cultural Responsiveness. In *Theories Bridging Ethnography and Evaluation* (Vol. 20, pp. 133-156). Emerald Group Publishing Limited.

70. Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), 1643-1669.

71. Calder, A. (2023). ISO 27001/ISO 27002: A guide to information security management systems.

72. Calder, A., & Watkins, S. (2024). IT governance: an international guide to data security and ISO 27001/ISO 27002.

73. Campino, J., Brochado, A., & Rosa, Á. (2021). Digital business transformation in the banking sector. In *Research Anthology on Concepts, Applications, and Challenges of FinTech* (pp. 186-215). IGI Global.

74. Carr, D. A. (2023). Mitigating fiscal risk through municipal cybersecurity. In *Research Handbook on City and Municipal Finance* (pp. 159-171). Edward Elgar Publishing.

75. Carreño, A. M. (2024). An Analytical Review of John Kotter's Change Leadership Framework: A Modern Approach to Sustainable Organizational Transformation. *Available at SSRN 5044428* .

76. Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *18*(2), 68-110.

77. Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, *28*(2), 1809-1831.

78. Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*.

79. Chakraborty, A., Biswas, A., & Khan, A. K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial Intelligence for Societal Issues* (pp. 3-25). Cham: Springer International Publishing.

80. Chakraborty, T., & Tripathi, M. (2024). and Upskilling Among Future Employees. *Revitalizing Student Skills for Workforce Preparation*, 37.

81. Chander, B., John, C., Warrier, L., & Gopalakrishnan, K. (2024). Toward trustworthy artificial intelligence (TAI) in the context of explainability and robustness. *ACM Computing Surveys*.

82. Chaudhary, K., & Alam, M. (2022). *Big data analytics: applications in business and marketing*. Auerbach Publications.

83. Chew, Y. C., & Mohamed Zainal, S. R. (2024). A Sustainable Collaborative Talent Management Through Collaborative Intelligence Mindset Theory: A Systematic Review. *SAGE Open*, *14*(2), 21582440241261851.

84. Chibo-Christopher, A. (2023). Digital Transformation and the Future of Work and Business in Africa.

85. Chiou, E. K., & Lee, J. D. (2023). Trusting automation: Designing for responsivity and resilience. *Human factors*, *65*(1), 137-165.

86. Chovarda, M. (2021). The Impact of Training & Development on Work Engagement: a study in the banking sector.

87. Christou, P. A. (2022). How to use thematic analysis in qualitative research. *Journal of Qualitative Research in Tourism*, *3*(2), 79-95.

88. Chugh, R., Macht, S., & Hossain, R. (2022). Robotic Process Automation: a review of organizational grey literature. *International Journal of Information Systems and Project Management*, *10*(1), 5-26.

89. Collins, A. (Ed.). (2022). *Contemporary security studies*. Oxford university press.

90. Constantino, S. M., Schlüter, M., Weber, E. U., & Wijermans, N. (2021). Cognition and behavior in context: a framework and theories to explain natural resource use decisions in social-ecological systems. *Sustainability Science*, *16*(5), 1651-1671.

91. Cornwell, N., Bilson, C., Gepp, A., Stern, S., & Vanstone, B. J. (2023). The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors. *Journal of the Operational Research Society*, *74*(1), 374-402.

92. Crumpler, W., & Lewis, J. A. (2022). *Cybersecurity Workforce Gap* (p. 10). Center for Strategic and International Studies (CSIS).

93. Cuthbertson, L. M., Robb, Y. A., & Blair, S. (2020). Theory and application of research principles and philosophical underpinning for a study utilising interpretative phenomenological analysis. *Radiography*, *26*(2), e94-e102.

94. Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. *Electronics*, *13*(5), 865.

95. Dagada, R. (2013, March). Digital banking security, risk and credibility concerns in South Africa. In *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)* (pp. 4-6). Kuala Lumpur Malaysia.

96. Dai, K., Kawaki, I. L., & Sakti, L. D. (2023). Mitigation of cyber security risk threats during the Covid-19 pandemic. *International Journal of Cyber and IT Service Management*, *3*(2), 107-119.

97. Dangal, M., & Joshi, R. (2020). Hermeneutic phenomenology: Essence in educational research. *Open Journal for Studies in Philosophy*, *4*(1).

98. Das, S., & Mukherjee, S. (2024). Navigating Cloud Security Risks, Threats, and Solutions for Seamless Business Logistics. In *Emerging*

Technologies and Security in Cloud Computing (pp. 252-275). IGI Global.

99. Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: first defense of an organizational security strategy.

100. Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications*, *73*, 103433.

101. Davenport, T. H., Harris, J. G., & Morison, R. (2010). *Analytics at work: Smarter decisions, better results*. Harvard Business Press.

102. De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920.

103. DeCrosta, J. (2021). *Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage* (Master's thesis, Utica College).

104. Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal*, *11*(1), 28.

105. Dhabliya, D., Ghule, G., Khubalkar, D., Moje, R. K., Kshirsagar, P. S., & Bendale, S. P. (2023). Robotic Process Automation in Cyber Security Operations: Optimizing Workflows with AI-Driven Automation. *Journal of Electrical Systems*, *19*(3).

106. Dillon, R., Lothian, P., Grewal, S., & Pereira, D. (2021). Cyber security: evolving threats in an ever-changing world. In *Digital Transformation in a Post-Covid World* (pp. 129-154). CRC Press.

107. Domoney, C. (2024). *Defending APIs: Uncover advanced defense techniques to craft secure application programming interfaces*. Packt Publishing Ltd.

108. Easttom, C. (2022). Quantum computing and cryptography. In *Modern Cryptography: Applied Mathematics for Encryption and Information Security* (pp. 397-407). Cham: Springer International Publishing.

109. Edwards, B. (2023). *In What Ways are Quality Assurance Professionals in England Responding to the Regulatory Changes Under the Higher Education and Research Act, 2017, and what are The Implications for the Quality Assurance of Higher Education Teaching and Learning? A Social Practice Approach* (Doctoral dissertation, Lancaster University (United Kingdom)).

110. Efe, A. (2023). A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Denetim ve Güvence Hizmetleri Dergisi*, *3*(2), 185-205.

111. Efijemue, O., Obunadike, C., Taiwo, E., Kizor, S., Olisah, S., Odooh, C., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customers data and preventing financial fraud in the United States financial sectors. *International Journal of Soft Computing*, *14*(3), 10-5121.

112. Emiliaty, A. (2024). Blockchain Technology: Revolutionizing Data Integrity and Security in Digital Environments. *Journal of Advanced Technological Innovations*, *1*(1), 1-8.

113. Enworo, O. C. (2023). Application of Guba and Lincoln's parallel criteria to assess trustworthiness of qualitative research on indigenous social protection systems. *Qualitative research journal*, *23*(4), 372-384.

114. Eulerich, M., Waddoups, N., Wagener, M., & Wood, D. A. (2024). The dark side of robotic process automation (RPA): Understanding risks and challenges with RPA. *Accounting Horizons*, *38*(2), 143-152.

115. Falk, J., Nolte, A., Huppenkothen, D., Weinzierl, M., Gama, K., Spikol, D., ... & Hayden, L. B. (2024). The future of hackathon research and practice. *IEEE Access*.

116. Familoni, B. T., & Onyebuchi, N. C. (2024). Advancements and challenges in AI integration for technical literacy: a systematic review. *Engineering Science & Technology Journal*, *5*(4), 1415-1430.

117. Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci*, *48*(2), 213-222.

118. Force, J. T. (2017). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Discussion Draft)* (No. NIST Special Publication (SP) 800-37 Rev. 2 (Draft)). National Institute of Standards and Technology.

119. Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer law & security review*, *41*, 105528.

120. Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian & New Zealand journal of psychiatry*, *36*(6), 717-732.

121. Frantti, T., & Jallow, M. (2023, August). Secure 3 rd party software integration. In *2023 10th International Conference on Dependable Systems and Their Applications (DSA)* (pp. 250-259). IEEE.

122. Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., ... & Benavides, E. (2022). Impact of social engineering attacks: A literature review. *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*, 25-35.

123. Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080.

124. Gajjar, V. R., & Taherdoost, H. (2024, April). Examining Cyber Threats and Vulnerabilities: A Deep Dive into British Columbia's Cybersecurity Landscape. In *2024 International Conference on Expert Clouds and Applications (ICOECA)* (pp. 240-245). IEEE.

125. Garane, A. S. (2024). An Assessment of Digital Transformation and Maturity in the South African banking sector.

126. George, A. S. (2024). Finance 4.0: The Transformation of Financial Services in the Digital Age. *Partners Universal Innovative Research Publication*, *2*(3), 104-125.

127. George, A. S. (2024). When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage. *Partners Universal Multidisciplinary Research Journal*, *1*(2), 134-152.

128. Gertze, L., & Petersen, F. (2024). Factors influencing the acceptance and use of a South African online bank. *South African Journal of Information Management*, *26*(1), 1759.

129. Gestin, M. (2024). *Privacy Preserving and fully-Distributed Identity Management Systems* (Doctoral dissertation, Universite de rennes 1).

130. Geyer, W., Richter, H., Fuchs, L., Frauenhofer, T., Daijavad, S., & Poltrock, S. (2001, September). A team collaboration space supporting capture and access of virtual meetings. In *Proceedings of the 2001 ACM International Conference on Supporting Group Work* (pp. 188-196).

131. Giuca, O., Popescu, T. M., Popescu, A. M., Prostean, G., & Popescu, D. E. (2021). A survey of cybersecurity risk management frameworks. In *Soft Computing Applications: Proceedings of the 8th International Workshop Soft Computing Applications (SOFA 2018), Vol. I 8* (pp. 240-272). Springer International Publishing.

132. Greenhalgh, T., Stramer, K., Bratan, T., Byrne, E., Mohammad, Y., & Russell, J. (2008). Introduction of shared electronic records: multi-site case study using diffusion of innovation theory. *Bmj*, *337*.

133. Grobler, Marthie, Raj Gaire, and Surya Nepal. "User, usage and usability: Redefining human centric cyber security." *Frontiers in big Data* 4 (2021): 583723.

134. Guan, A., & Chen, C. M. (2022). A novel verification scheme to resist online password guessing attacks. *IEEE Transactions on Dependable and Secure Computing*, *19*(6), 4285-4293.

135. Gumede, S., & Manenzhe, P. (2023). Competition regulation for digital markets: The South African experience. *The African Journal of Information and Communication*, *2023*(31), 1-19.

136. Gupta, A. (2024). *Qualitative Methods and Data Analysis Using ATLAS. ti*. New York: Springer International Publishing.

137. Hakizimana, S., Wairimu, M. M. C., & Stephen, M. (2023). Digital Banking Transformation and Performance-Where Do We Stand?. *International Journal of Management Research and Emerging Sciences*, *13*(1).

138. Haleem, A., Javaid, M., Singh, R. P., Rab, S., & Suman, R. (2021). Hyperautomation for the enhancement of automation in industries. *Sensors International*, *2*, 100124.

139. Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), 41-59.

140. Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and

regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

141. Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage.

142. Holmes, A. E. (2021). *Exploring the Challenges of the Risk Management Framework Implementation for Cybersecurity Professionals* (Doctoral dissertation, Northcentral University).

143. Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk*. John Wiley & Sons.

144. Iacovidou, E., Hahladakis, J. N., & Purnell, P. (2021). A systems thinking approach to understanding the challenges of achieving the circular economy. *Environmental Science and Pollution Research*, *28*, 24785-24806.

145. Iannone, E., Di Nucci, D., Sabetta, A., & De Lucia, A. (2021, May). Toward automated exploit generation for known vulnerabilities in open-source libraries. In *2021 IEEE/ACM 29th International Conference on Program Comprehension (ICPC)* (pp. 396-400). IEEE.

146. Ibiyemi, M. O., & Olutimehin, D. O. (2024). Cybersecurity in supply chains: Addressing emerging threats with strategic measures. *International Journal of Management & Entrepreneurship Research*, *6*(6).

147. Ibrahim, H. (2022). A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), 50-68.

148. Imran, H., Salama, M., Turner, C., & Fattah, S. (2022, March). Cybersecurity risk management frameworks in the oil and gas sector: A systematic literature review. In *Future of Information and Communication Conference* (pp. 871-894). Cham: Springer International Publishing.

149. Irshaidat, R. (2022). Interpretivism vs. positivism in political marketing research. *Journal of Political Marketing*, *21*(2), 126-160.

150. Islam, M. R. (2024). *Generative AI, Cybersecurity, and Ethics*. John Wiley & Sons.

151. Islam, M., Bohuk, M. S., Chung, P., Ristenpart, T., & Chatterjee, R. (2023). {Araña}: Discovering and Characterizing Password Guessing Attacks in Practice. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 1019-1036).

152. Jackson, W., & Harlee, M. (2024). Human Error and Cybersecurity in SMEs: Tailored Training Programs for a Safer Digital Environment.

153. Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527-565.

154. Jain, N. (2021). Survey versus interviews: Comparing data collection tools for exploratory research. *The Qualitative Report*, *26*(2), 541-554.

155. Jaiwant, S. V. (2022). Artificial intelligence and personalized banking. In *Handbook of Research on Innovative Management Using AI in Industry 5.0* (pp. 74-87). IGI Global.

156. James, C. (2023). Securing Bot Credentials and Sensitive Information in Robotic Process Automation (RPA).

157. Jana, D. S., Khedkar, A. E., & Khedkar, C. E. (2021). Digital Banking: The Future of Banking. *Vidyabharati International Interdisciplinary Research Journal*, *12*(2), 281-284.

158. Jansawang, N., Insumran, Y., & Kenaphoom, S. (2025). Quality Assurance for Lifelong Education: A Comprehensive Review. *ONESQA Quality Assurance in Education Journal*, *1*(1), 1-19.

159. Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in cybersecurity management* (pp. 139-161). Cham: Springer International Publishing.

160. Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(6), e1418.

161. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, 564-574.

162. Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171.

163. John, E. I., Effanga Effanga Okon, M. E. N., & John, O. (2022). A class of ratio-cum-product estimators of population mean under extreme ranked set sampling (ERSS) and simple random sampling (SRS).

164. Johnson, M., Jain, R., Brennan-Tonetta, P., Swartz, E., Silver, D., Paolini, J., ... & Hill, C. (2021). Impact of big data and artificial intelligence on industry: developing a workforce roadmap for a data driven economy. *Global Journal of Flexible Systems Management*, *22*(3), 197-217.

165. Jonnalagadda, A. M. C. (2024). A SYSTEMATIC ANALYSIS OF SECURITY CHALLENGES IN ENTERPRISE CLOUD DEPLOYMENTS: UNDERSTANDING THE SHARED RESPONSIBILITY MODEL AND RISK MITIGATION STRATEGIES. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET)*, *15*(6), 535-547.

166. Jordan, C. A. (2022). *Exploring the Cybersecurity Skills Gap: A Qualitative Study of Recruitment and Retention from a Human Resource Management Perspective*. Northcentral University.

167. Jung, B., Han, I., & Lee, S. (2001). Security threats to Internet: a Korean multi-industry investigation. *Information & Management*, *38*(8), 487-498.

168. Jung, D., Dorner, V., Glaser, F., & Morana, S. (2018). Robo-advisory: digitalization and automation of financial advisory. *Business & Information Systems Engineering*, *60*, 81-86.

169. Jurczuk, A., & Florea, A. (2022). Future-oriented digital skills for process design and automation. *Human Technology*, *18*(2), 122-142.

170. Kabalina, V., & Osipova, A. (2022). Identifying and assessing talent potential for future needs of a company. *Journal of Management Development*, *41*(3), 147-162.

171. Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for windows based ransomware attacks. *Expert Systems with Applications*, *190*, 116198.

172. Karakasilioti, G. M. (2024). *Supporting the digital operational resilience of the financial sector: the EU's DORA Digital Operational Resilience Act* (Master's thesis, Πανεπιστήμιο Πειραιώς).

173. Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, *26*(2), 107.

174. Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys (CSUR)*, *54*(11s), 1-35.

175. Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(8), 1-21.

176. Kebede, Amarech, Amare Asgedom, and Abraha Asfaw. "Is linking technical and vocational training with industry a bridge to employability? Lessons from a literature review for Ethiopia." *Cogent Education* 11, no. 1 (2024): 2406721.

177. Kemendi, A., & Michelberger, P. (2024). Process security methods and measurement in the context of standard management systems. *Engineering Management in Production and Services*, *16*(2), 148-165.

178. Khabouze, R. (2022). *Modernization of Legacy Information Technology Systems* (Doctoral dissertation, Walden University).

179. Khan, H. U., Sohail, M., Nazir, S., Hussain, T., Shah, B., & Ali, F. (2023). Role of authentication factors in Fin-tech mobile transaction security. *Journal of Big Data*, *10*(1), 138.

180. Khan, I. (2023). Ai-powered data governance: ensuring integrity in banking's technological frontier.

181. Khanboubi, F., & Boulmakoul, A. (2019). Digital transformation in the banking sector: Surveys exploration and analytics. *International Journal of Information Systems and Change Management*, *11*(2), 93-127.

182. Khatoon, A., & Riaz, R. (2025). Quantum Computing Impacts on Smart City Cybersecurity Through Resilient Defense Framework: Quantum Computing Impacts on Resilient Cybersecurity Frameworks for Smart Cities. *Ubiquitous Technology Journal*, *1*(1), 23-31.

183. Kircher, R., & Zipp, L. (2022). Questionnaires to elicit quantitative data. *Research methods in language attitudes*, 129-144.

184. Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a risk analysis strategy framework for impact assessment in information security management systems: A case study in it consulting industry. *Sustainability*, *14*(3), 1269.

185. Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. *Sustainability*, *15*(7), 5828.

186. Klosowski, T. (2021). The state of consumer data privacy laws in the US (and why it matters). *New York Times*.

187. Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.

188. Knotter, L. (2022). Interpretivism in international relations research. In *Handbook of Research Methods in International Relations* (pp. 629-650). Edward Elgar Publishing.

189. Koenaite, M., Maziriri, E., & Chuchu, T. (2021). Attitudes towards utilising mobile banking applications among Generation Z consumers in South Africa. *Journal of Business and Management Review*, *2*(6), 417-438.

190. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. *Sage Open*, *11*(3), 21582440211047576.

191. Krishnan, C., Gupta, A., Gupta, A., & Singh, G. (2022). Impact of artificial intelligence-based chatbots on customer engagement and business growth. In *Deep learning for social media data analytics* (pp. 195-210). Cham: Springer International Publishing.

192. Kshetri, N. (2021). Blockchain technology for improving transparency and citizen's trust. In *Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1* (pp. 716-735). Springer International Publishing.

193. Kumah, P., Yaokumah, W., & Asante-Offei, K. O. (2024). The role of skills, processes and technology in information security risk management. *International Journal of Business Continuity and Risk Management*, *14*(4), 392-412.

194. Kumar, I. (2023). Emerging threats in cybersecurity: a review article. *International Journal of Applied and Natural Sciences*, *1*(1), 01-08.

195. Kumar, S., Khanna, S., Ghosh, N., & Kumar, S. O. D. (2023). Importance of Artificial Intelligence (AI) and Robotic Process Automation (RPA) in the Banking Industry: A Study from an Indian Perspective. In *Confluence of Artificial Intelligence and Robotic Process Automation* (pp. 231-266). Singapore: Springer Nature Singapore.

196. Kuraku, D. S., Kalla, D., Smith, N., & Samaah, F. (2023). Safeguarding FinTech: Elevating Employee Cybersecurity Awareness in Financial Sector. *International Journal of Applied Information Systems (IJAIS)*, *12*(42).

197. Lakens, D. (2022). Sample size justification. *Collabra: psychology*, *8*(1), 33267.

198. Leal Filho, W., Dibbern, T., Dinis, M. A. P., Cristofoletti, E. C., Mbah, M. F., Mishra, A., ... & Aina, Y. A. (2024). The added value of partnerships in implementing the UN sustainable development goals. *Journal of Cleaner Production*, *438*, 140794.

199. Lebaea, R., Roshe, Y., Ntontela, S., & Thango, B. A. (2024). The Role of Data Governance in Ensuring System Success and Long-Term IT Performance: A Systematic.

200. Lee, G.J., & Armstrong, B. (2023). Introduction to Digital Business & Technology. 3rd Edition by Silk Route Press.

201. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.

202. Lee, S. B. (2020). Chatbots and communication: The growing role of artificial intelligence in addressing and shaping customer needs. *Business Communication Research and Practice*, *3*(2), 103-111.

203. Lekhelebana, L. G. (2022). *Credit risk management impact on loan performance in development finance institutions in South Africa* (Doctoral dissertation, Doctoral dissertation, Nelson Mandela University). http://vital. seals. ac. za: 8080/vital/access/manager/Repository/vital: 58217).

204. Lewis, C. (2005). Negotiating the net: the internet in South Africa (1990-2003). *Lewis, C (2005)'Negotiating the Net: The Internet in South Africa (1990–2003), Information Technologies and International Development*, *2*(3), 1-28.

205. Li, L. (2022). Reskilling and upskilling the future-ready workforce for industry 4.0 and beyond. *Information Systems Frontiers*, 1-16.

206. Lim, W. M. (2024). What Is Qualitative Research? An Overview and Guidelines. *Australasian Marketing Journal*, 14413582241264619.

207. Lim, W. M. (2025). What is qualitative research? An overview and guidelines. *Australasian Marketing Journal*, *33*(2), 199-229.

208. Liu, F., Cui, Y., Masouros, C., Xu, J., Han, T. X., Eldar, Y. C., & Buzzi, S. (2022). Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond. *IEEE journal on selected areas in communications*, *40*(6), 1728-1767.

209. Liu, Q., Zeng, H., Wang, T., Ni, H., Li, Y., Qian, W., ... & Xu, G. (2024). Development of RPA-Cas12a assay for rapid and sensitive detection of Pneumocystis jirovecii. *BMC microbiology*, *24*(1), 314.

210. Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IoT world. *Security and Privacy*, *6*(6), e318.

211. Lottu, O. A., Abdul, A. A., Daraojimba, D. O., Alabi, A. M., John-Ladega, A. A., & Daraojimba, C. (2023). Digital transformation in banking: a review of Nigeria's journey to economic prosperity. *International Journal of Advanced Economics*, *5*(8), 215-238.

212. Loureiro, S. (2021). Security misconfigurations and how to prevent them. *Network Security*, *2021*(5), 13-16.

213. Louw, C., & Nieuwenhuizen, C. (2020). Digitalisation strategies in a South African banking context: A consumer services analysis. *South African Journal of Information Management*, *22*(1), 1-8.

214. Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*, *69*, 43-51.

215. Madakam, S., Holmukhe, R. M., & Jaiswal, D. K. (2019). The future digital work force: robotic process automation (RPA). *JISTEM-Journal of Information Systems and Technology Management*, *16*, e201916001.

216. Madasamy, S. (2022). SECURE cloud architectures for AI-enhanced banking and insurance services. *International Research Journal of Modernization in Engineering Technology and Science*, *4*, 6345-6353.

217. Maddireddy, B. R., & Maddireddy, B. R. (2023). Automating Malware Detection: A Study on the Efficacy of AI-Driven Solutions. *Journal Environmental Sciences And Technology*, *2*(2), 111-124.

218. Magasi, C. (2021). The role of transformational leadership on employee performance: A perspective of employee empowerment. *European Journal of Business and Management Research*, *6*(6), 21-28.

219. Mahalakshmi, V., Kulkarni, N., Kumar, K. P., Kumar, K. S., Sree, D. N., & Durga, S. (2022). The role of implementing Artificial Intelligence and Machine Learning technologies in the financial services Industry for creating competitive intelligence. *Materials Today: Proceedings*, *56*, 2252-2255.

220. Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *NIPES-Journal of Science and Technology Research*, *6*(2).

221. Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69.

222. Maniraj Singh, A. (2004, June). Trends in South African internet banking. In *Aslib Proceedings* (Vol. 56, No. 3, pp. 187-196). Emerald Group Publishing Limited.

223. Manser Payne, E. H., Peltier, J., & Barger, V. A. (2021). Enhancing the value co-creation process: artificial intelligence and mobile banking service platforms. *Journal of Research in Interactive Marketing*, *15*(1), 68-85.

224. Markonda, S. M., & Pannala, S. P. R. (2023). From Software Engineer to being a Machine Learning Engineer-A Study on Skills and Responsibilities.

225. Martin, P. (2023). *Insider risk and personnel security: An introduction*. Taylor & Francis.

226. Masheleni, C. I. (2022). Fourth industrial banking: case studies into digitising banking models and the foreseeable effects in South Africa.

227. McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., ... & Halgamuge, M. N. (2024). From cobit to iso 42001: Evaluating

cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security*, 103964.

228. Melnyk, V. (2024). Transforming the nature of trust between banks and young clients: from traditional to digital banking. *Qualitative Research in Financial Markets*, *16*(4), 618-635.

229. Miller, J. (2024). Enhancing Educators' Cultural and Digital Literacies through Makerspace Development Activities. In *STEM Education-Recent Developments and Emerging Trends*. IntechOpen.

230. Mishra, A. (2022). *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition)*. BPB Publications.

231. Mitchell, G. J., & Cody, W. K. (1993). The role of theory in qualitative research. *Nursing Science Quarterly*, *6*(4), 170-178.

232. Mittal, M., Kumar, K., & Behal, S. (2023). Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft computing*, *27*(18), 13039-13075.

233. Mkele, Z. (2024). *The Impact of the Entry of Capitec Bank on Competition in the South African Banking Sector* (Master's thesis, University of Johannesburg (South Africa)).

234. MODE, M. M. (2023). Diagrammatic Representation of the Central Tendency. *STATISTICS AND DATA INTERPRETATION IN EDUCATIONAL RESEARCH*, 130.

235. Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of economic development, environment and people*, *7*(1), 23-48.

236. Mohammad, S. M., & Surya, L. (2018). Security automation in Information technology. *International journal of creative research thoughts (IJCRT)–Volume*, *6*.

237. Molinillo, S., & Japutra, A. (2017). Organizational adoption of digital information and technology: a theoretical review. *The Bottom Line*, *30*(01), 33-46.

238. Molopyane, M. (2021). Impact of current technologies on jobs and employment: Insights from mining and banking in South Africa. *Leap 4.0: African Perspectives on the Fourth Industrial Revolution*, 219.

239. Momani, D. A. M. (2024). The Role of IT Governance in Organizations: Best Practices for Enhancing Audit, Control, and Success. *Available at SSRN 5053120*.

240. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1-9.

241. Montgomery, T., & Baglioni, S. (2021). Defining the gig economy: platform capitalism and the reinvention of precarious work. *International Journal of Sociology and Social Policy*, *41*(9/10), 1012-1025.

242. Morandini, S., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D., & Pietrantoni, L. (2023). The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. *Informing Science*, *26*, 39-68.

243. Morgan, J. (2014). *The future of work: Attract new talent, build better leaders, and create a competitive organization*. John Wiley & Sons.

244. Moser, S., & Bader, C. (2023). Why do people participate in grassroots sustainability initiatives? Different motives for different levels of involvement. *Frontiers in Sustainability*, *3*, 994881.

245. Motulsky, S. L. (2021). Is member checking the gold standard of quality in qualitative research?. *Qualitative Psychology*, *8*(3), 389.

246. Mphahlele, T. (2024). Developing a cybersecurity framework for commercial banks in South Africa.

247. Muir, A., Brown, K., & Girma, A. (2024, November). Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks. In *Proceedings of the Future Technologies Conference* (pp. 597-607). Cham: Springer Nature Switzerland.

248. Mujinga, M. (2024). Online Banking User Experience: A User Experience Questionnaire (UEQ) Assessment in South Africa. *Indonesian Journal of Information Systems*, *6*(2), 117-129.

249. Mullet, V., Sondi, P., & Ramat, E. (2021). A review of cybersecurity guidelines for manufacturing factories in industry 4.0. *IEEE Access*, *9*, 23235-23263.

250. Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International review of financial analysis*, *81*, 102103.

251. Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2024). Demystification and actualisation of data saturation in qualitative research through thematic analysis. *International Journal of Qualitative Methods*, *23*, 16094069241229777.

252. Naidoo, A. (2021). *The Influence of Digitalization on Work and Employment in the Banking Sector in South Africa* (Doctoral dissertation).

253. Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, *59*, 102334.

254. Nash, I. (2021). Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices. *Computer Law & Security Review*, *40*, 105529.

255. Nel, J., & Boshoff, C. (2021). Traditional-bank customers' digital-only bank resistance: evidence from South Africa. *International Journal of Bank Marketing*, *39*(3), 429-454.

256. Nguyen, M. T., & Tran, M. Q. (2023). Balancing security and privacy in the digital age: an in-depth analysis of legal and regulatory frameworks impacting cybersecurity practices. *International Journal of Intelligent Automation and Computing*, *6*(5), 1-12.

257. Nicoletti, B., & Nicoletti, B. (2021). Protection of Banking 5.0. *Banking 5.0: How Fintech Will Change Traditional Banks in the'New Normal'Post Pandemic*, 401-430.

258. Nizami, N., Tripathi, T., & Mohan, M. (2022). Transforming skill gap crisis into opportunity for upskilling in India's IT-BPM sector. *The Indian Journal of Labour Economics*, *65*(3), 845-862.

259. Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

260. Nof, S. Y. (2009). Automation: What it means to us around the world. *Springer handbook of automation*, 13-52.

261. Nwankwo, I., Stauch, M., Radoglou-Grammatikis, P., Sarigiannidis, P., Lazaridis, G., Drosou, A., & Tzovaras, D. (2022). Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector. *Electronics*, *11*(6), 965.

262. O'Hagan, L. (2023). The Human Element of Data Exploitation.

263. O'Kane, P., Smith, A., & Lerman, M. P. (2021). Building transparency and trustworthiness in inductive research through computer-aided qualitative data analysis software. *Organizational Research Methods*, *24*(1), 104-139.

264. Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N. L., Onunka, O., & Omotosho, A. (2023). Mitigating cybersecurity risks in the US healthcare sector. *International Journal of Research and Scientific Innovation (IJRSI)*, *10*(9), 177-193.

265. Oladele, T. C. (2024). Digital Transformation in Finance and Banking Sectors. In *Digital Transformation in South Africa: Perspectives from an Emerging Economy* (pp. 23-38). Cham: Springer Nature Switzerland.

266. Oladipo, J. O., Okoye, C. C., Elufioye, O. A., Falaiye, T., & Nwankwo, E. E. (2024). Human factors in cybersecurity: Navigating the fintech landscape. *International Journal of Science and Research Archive*, *11*(1), 1959-1967.

267. Omarini, A. (2017). The digital transformation in banking and the role of FinTechs in the new financial intermediation scenario.

268. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

269. Onih, V. A., Sevidzem, Y. S., & Adeniji, S. (2024). The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures. *International Journal of Scientific and Management Research*.

270. Osborne, N., & Grant-Smith, D. (2021). In-depth interviewing. In *Methods in urban analysis* (pp. 105-125). Singapore: Springer Singapore.

271. Owusu, S. (2023). *Bridging the Cybersecurity Workforce Skill Gap With Experiential Learning: The Role of Cybersecurity Clinics* (Doctoral dissertation, Marymount University).

272. Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643.

273. Pace, D. S. (2021). Probability and non-probability sampling-an entry point for undergraduate researchers. *International Journal of Quantitative and Qualitative Research Methods*, *9*(2), 1-15.

274. Padma, S. (2024). Learning Dynamics, Employee Performance and Retention: A Bibliometric Analysis in the Service Sector.

275. Parker, S. K., & Grote, G. (2022). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world. *Applied psychology*, *71*(4), 1171-1204.

276. Parry, A., Orkoh, E., Jansen van Rensburg, S. J., & Viviers, W. (2024). Digital developments and employment: Understanding trends in Africa.

277. Patel, K. (2023). Credit card analytics: a review of fraud detection and risk assessment techniques. *International Journal of Computer Trends and Technology*, *71*(10), 69-79.

278. Patel, Kathan, and Dhaval Chudasama. "National security threats in cyberspace." *National Journal of Cyber Security Law* 4, no. 1 (2021): 12-20p.

279. Pedro, B. (2024). *Building an API Product: Design, implement, release, and maintain API products that meet user needs*. Packt Publishing Ltd.

280. Perera, S., Jin, X., Maurushat, A., & Opoku, D. G. J. (2022, March). Factors affecting reputational damage to organisations due to cyberattacks. In *Informatics* (Vol. 9, No. 1, p. 28). MDPI.

281. Pérez-Morón, J. M., García Alonso, R., & Thoene, U. (2024). Looking back to move forward: shedding light on the dark side of entrepreneurship. *New England Journal of Entrepreneurship*, *27*(2), 152-172.

282. Pervin, N., & Mokhtar, M. (2022). The interpretivist research paradigm: A subjective notion of a social context. *International Journal of Academic Research in Progressive Education and Development*, *11*(2), 419-428.

283. Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., & Bonders, M. (2023, July). CyberEscape approach to advancing hard and soft skills in cybersecurity education. In *International Conference on Human-Computer Interaction* (pp. 441-459). Cham: Springer Nature Switzerland.

284. Polis, G. (2023). *Using the principles of cybersecurity ethics to mitigate cybersecurity risks* (Doctoral dissertation, Masters thesis. Banku Augstskola School of Business and Finance. Available at: doi: 10.13140/RG. 2.2. 15285.86245).

285. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371-390.

286. Prakash, S., Venkatasubbu, S., & Konidena, B. K. (2023). Unlocking insights: AI/ML applications in regulatory reporting for US banks. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *1*(1), 177-184.

287. Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247.

288. Prastyanti, R. A., Rezi, R., & Rahayu, I. (2023). Ethical Fintech is a New Way of Banking. *Kontigensi: Jurnal Ilmiah Manajemen*, *11*(1), 255-260.

289. Preetam, S. (2022). *Behavioural analytics for threat detection* (Master's thesis, Universitat Politècnica de Catalunya).

290. Pugnetti, Carlo, and Carlos Casián. "Cyber risks and swiss smes: an investigation of employee attitudes and behavioral vulnerabilities." (2021).

291. Qazi, F. (2022). Application Programming Interface (API) Security in Cloud Applications. *EAI Endorsed Transactions on Cloud Systems*, *7*(23), e1-e1.

292. Rahul, R., Geetha, S., Priyatharsini, S., Mehata, K., Sundaresan Perumal, T., Ethiraj, N., & Sendilvelan, S. (2024). Cybersecurity Issues and Challenges in Quantum Computing. *Topics in Artificial Intelligence Applied to Industry 4.0*, 203-221.

293. Rawal, B. S., Manogaran, G., & Peter, A. (2023). *Cybersecurity and Identity Access Management*. Singapore: Springer.

294. Renjith, V., Yesodharan, R., Noronha, J. A., Ladd, E., & George, A. (2021). Qualitative methods in health care research. *International journal of preventive medicine*, *12*(1), 20.

295. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.

296. Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). AI in the financial sector: The line between innovation, regulation and ethical responsibility. *Information*, *15*(8), 432.

297. Roberts, R. E. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. *Qualitative Report*, *25*(9).

298. Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*, *178*, 121562.

299. Rogge, A., Anter, L., Kunze, D., Pomsel, K., & Willenbrock, G. (2024). Standardized sampling for systematic literature reviews (STAMP method): ensuring reproducibility and replicability. *Media and Communication*, *12*.

300. Roseline, S. A., & Geetha, S. (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers & Electrical Engineering*, *92*, 107143.

301. Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in pharmacy teaching and learning*, *8*(4), 509-516.

302. Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer communications*, *169*, 179-201.

303. Sanmath, A. (2019). Fin Tech Banking–The Revolutionized Digital Banking. *International Journal of Trend in Scientific Research and Development*, *1*(1), 17-20.

304. Santana, M., & Cobo, M. J. (2020). What is the future of work? A science mapping analysis. *European Management Journal*, *38*(6), 846-862.

305. Sargiotis, D. (2024). Data Security and privacy: protecting sensitive information. In *Data governance: a guide* (pp. 217-245). Cham: Springer Nature Switzerland.

306. Sarkar, G., Singh, H., Kumar, S., & Shukla, S. K. (2023, August). Tactics, techniques and procedures of cybercrime: A methodology and tool for cybercrime investigation process. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-10).

307. Sarker, I. H. (2024). *AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability*. Springer Nature.

308. Saxena, P., Saxena, V., Pandey, A., Flato, U., & Shukla, K. (2023). *Multiple aspects of artificial intelligence*. Book Saga Publications.

309. Selvaganapathy, S., Sadasivam, S., & Ravi, V. (2021). A review on android malware: Attacks, countermeasures and challenges ahead. *Journal of Cyber Security and Mobility*, 177-230.

310. Seth, D., Nerella, H., Najana, M., & Tabbassum, A. (2024). Navigating the Multi-cloud Maze: benefits, challenges, and Future trends. *International Journal of Global Innovations and Solutions (IJGIS)*.

311. Shahraki, A. S., Peszynski, K., Barua, B., Kondylas, L., & Breteler, A. (2022). Digital skills and cyber security. How do we secure our future?.

312. Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. *World Journal of Advanced Research and Reviews*, *15*(1), 138-156.

313. Sharma, L. R. (2023). Choosing appropriate probability sampling designs in research. *Health*, *2*, 4-21.

314. Shepherd, A. J. (2021). *The EU security continuum: Blurring Internal and External security*. Routledge.

315. Shetty, G. (2022). Job Loss due to Automation Technologies: Perceptions of Fairness in the Information Technology Sector of India. *OPUS: HR Journal*, *12*(2), 2021.

316. Shidaganti, G., Khandelwal, L., Gupta, K., & Vaswani, H. (2023). Challenges in Banking and Solving Them Using RPA. In *Confluence of Artificial Intelligence and Robotic Process Automation* (pp. 133-156). Singapore: Springer Nature Singapore.

317. Shikhaliyev, R. (2024). Cybersecurity risks management of industrial control systems: A review. *Problems of Information Technology*, 37-43.

318. SHRM. (2023, December 21). What is meant by “the future of work”? *SHRM*. https://www.shrm.org/topics-tools/tools/hr-answers/meant-the-future-work

319. Shwedeh, F., Malaka, S., & Rwashdeh, B. (2023). The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review. *Migration Letters*, *20*(S9), 1066-1072.

320. Sibeko, S. (2023). *Digital transformation strategies in the South African banking sector* (Master's thesis, University of the Witwatersrand, Johannesburg (South Africa)).

321. Siedlecki, S. L. (2022). Conducting interviews for qualitative research studies. *Clinical Nurse Specialist*, *36*(2), 78-80.

322. Smit, B. (2021). Introduction to ATLAS. ti for Mixed Analysis. In *The Routledge Reviewer’s Guide to Mixed Methods Analysis* (pp. 331-342). Routledge.

323. Spielman, Z. A., Remer, S. J., Lilleng, T., Droivoldsmo, A., & Mydland, Ø. (2024). *Integrated Operations in Nuclear: A Strategic Approach Addressing Workforce Attraction and Knowledge Retention* (No. INL/RPT-24-80098-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (United States).

324. Stalmeijer, R. E., Brown, M. E., & O'Brien, B. C. (2024). How to discuss transferability of qualitative research in health professions education. *The Clinical Teacher*, e13762.

325. Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection*, *37*, 100505.

326. Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762.

327. Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE access*, *10*, 39325-39343.

328. Taavitsainen, N. (2025). Trust to Exploitation: The Legal and Societal Implications of Payment Fraud and the Path Toward Stronger Protections.

329. Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), 2181.

330. Taherdoost, H. (2022). What are different research approaches? Comprehensive Review of Qualitative, quantitative, and mixed method

research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, *5*(1), 53-63.

331. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28), e3-e3.

332. Tenny, S., Brannan, J. M., & Brannan, G. D. (2017). Qualitative study.

333. Teodorescu, D., Ingram, C., & Oliver, T. (2024). Ensuring a Sustainable STEM Sector in the US: The Role of Culturally Responsive Mentoring in Undergraduate Education. *Sustainability*, *16*(17), 7775.

334. Thakur, M. (2024). Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1-20.

335. Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, 104130.

336. Thishopana, B., & Arulrajah, A. A. (2023). Navigating the Digital Frontier: Challenges Faced by Bank Employees in Embracing Digital Banking. *IUP Journal of Bank Management*, *22*(2).

337. Thomas, G., & Sule, M. J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1), 18-40.

338. Toropov, R. (2025). Securing Privileged Access: Best Practices for PAM System Implementation.

339. Toth, R., & Erdődi, L. (2023, November). Expanding Horizons: The Evolving Landscape of Development Opportunities in Cybersecurity Training Platforms. In *Norsk IKT-konferanse for forskning og utdanning* (No. 3).

340. Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, *5*(3), 32.

341. Tschang, F. T., & Almirall, E. (2021). Artificial intelligence as augmenting automation: Implications for employment. *Academy of Management Perspectives*, *35*(4), 642-659.

342. Tshabalala, L. (2021). *Commercial segment competitiveness in a market disrupted by digital banks in South Africa* (Doctoral dissertation).

343. Tzafestas, S. G. (2010). Human and nature minding automation. *Automation, Human, Nature and Development*.

344. Uba, T., Ikughur, A. J., & Nwaosu, S. C. (2021). An Alternative Hybrid Estimator of Finite Population Mean in Simple Random Sampling. *Asian Journal of Probability and Statistics*, *15*(4), 276-298.

345. Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(3), 382-409.

346. Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(3), 382-409.

347. Umar, S. (2022). Innovative banking, the unbanked and domestic savings in South Africa.

348. Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, *11*(1), 1810-1817.

349. Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis.

350. Valdez, V. B., & Javier, S. P. (2021). Digital divide: from a peripheral to a core issue for all SDGs. In *Reduced Inequalities* (pp. 88-101). Cham: Springer International Publishing.

351. Van Hoa, N., & Van Thu, P. (2024). Factors Affecting Talent Attraction: Theoretical Basis. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(1), 865-869.

352. Van Manen, M. (2017). Phenomenology in its original sense. *Qualitative health research*, *27*(6), 810-825.

353. Villar, A. S., & Khan, N. (2021). Robotic process automation in banking industry: a case study on Deutsche Bank. *Journal of Banking and Financial Technology*, *5*(1), 71-86.

354. Vinodh, S., Antony, J., Agrawal, R., & Douglas, J. A. (2021). Integration of continuous improvement strategies with Industry 4.0: a systematic review and agenda for further research. *The TQM Journal*, *33*(2), 441-472.

355. Wai, E., & Lee, C. K. M. (2023). Seamless Industry 4.0 Integration: A Multilayered Cyber-Security Framework for Resilient SCADA Deployments in CPPS. *Applied Sciences*, *13*(21), 12008.

356. Walsh, M., Worrell, C., & Scanlon, T. (2024). Toward Use of Artificial Intelligence for Advanced Persistent Threat Detection.

357. Wan, Y., & Cao, J. (2023). A Brief Survey of Recent Advances and Methodologies for the Security Control of Complex Cyber–Physical Networks. *Sensors*, *23*(8), 4013.

358. Wang, Y., Wang, C., Gu, C., Cui, Y., O'Neill, M., & Liu, W. (2022). A generic dynamic responding mechanism and secure authentication

protocol for strong PUFs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *30*(9), 1256-1268.

359. Wani, T. A., & Ali, S. W. (2015). Innovation diffusion theory. *Journal of general management research*, *3*(2), 101-118.

360. Wejnert, B. (2002). Integrating models of diffusion of innovations: A conceptual framework. *Annual review of sociology*, *28*(1), 297-326.

361. Welch, C., Piekkari, R., Plakoyiannaki, E., & Paavilainen-Mäntymäki, E. (2020). Theorising from case studies: Towards a pluralist future for international business research. *Research methods in international business*, 171-220.

362. Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, *12*(3), 546.

363. West, D. M. (2018). *The future of work: Robots, AI, and automation*. Brookings Institution Press.

364. Widodo, A. M., Pappachan, P., Sekti, B. A., Anwar, N., Widayanti, R., Rahaman, M., & Bansal, R. (2024). Quantum-Resistant Cryptography. In *Innovations in Modern Cryptography* (pp. 100-130). IGI Global.

365. William, P., et al. "Future of Digital Work Force in Robotic Process Automation." *Robotic Process Automation* (2023): 297-314.

366. Wittkop, J. (2022). *The cybersecurity playbook for modern enterprises: an end-to-end guide to preventing data breaches and cyber attacks*. Packt Publishing Ltd.

367. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and

recommendations. *International Journal of Information Security*, *21*(1), 115-158.

368. Yong Wong, M., Landen, M., Antonakakis, M., Blough, D. M., Redmiles, E. M., & Ahamad, M. (2021, November). An inside look into the practice of malware analysis. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3053-3069).

369. Yulianto, S., & Soewito, B. (2023, October). Envisioning Risk Management for Smart Contracts: A Conceptual Model. In *2023 International Conference on Informatics Engineering, Science & Technology (INCITEST)* (pp. 1-7). IEEE.

370. Zaid, T., & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, *7*.

371. Zaydi, M. (2024). A new framework for agile cybersecurity risk management. *Agile Security in the Digital Era: Challenges and Cybersecurity Trends*, *19*.

372. Zimmermann, O., Stocker, M., Lubke, D., Zdun, U., & Pautasso, C. (2022). *Patterns for API design: simplifying integration with loosely coupled message exchanges*. Addison-Wesley Professional.

373. Σαμπάνης, Σ. (2024). Analysis of framework methods and software tools for information security risk management.

APPENDIX A (Tables)

Theme-Category Codebook for Theme 1.

Research Question 1	Theme	Category	Example of quotation
What are the cybersecurity threats posed by automation technologies of the future of work in digital banking?	Cybersecurity Risks.	Area	"*Also, I would say staff training (or lack thereof). Regardless of how strong your cyber security is, if the staff continuously opens and clicks on foreign links, the company will be breached. Banks, however, are starting to have regular training and advise employees about cyber-attacks.*"
		Vulnerability	*"I would say AI and Machine Learning Exploits. This includes Adversarial Attacks, Data Poisoning and Model Theft. Adversarial Attacks: Attackers can feed deliberately crafted inputs to AI systems to confuse them, such as bypassing fraud detection by exploiting patterns in machine*

			learning models."
		Exploit	*"In my experience, attackers can exploit vulnerabilities in automated banking systems through API Security Risks, which involve API key theft, SQL injection, and Cross-Site Scripting (XSS)."*

Table 1A: Theme-Category codebook of Theme 1.

Theme-Category Codebook for Theme 1.

Theme	Category	Codes	Description
Cybersecurity Risks.	AREA	AI-Powered Security Solution	This code represents instances where participants discuss how an area might be more susceptible to compromise.
		API Security Best Practices	Participants recognise an area.
		Data Privacy & Protection	Participants reported an area.
		Employee Training & Awareness	Participants reported an area more susceptible to compromise.
		Incident Response planning	Participants discuss an area.
		Integration Points	Participants reported an area.
		Regulatory Reporting	Participants discuss an area more susceptible to compromise.
		Robust security Framework	Participants recognise an area.
		RPA Security	Participants recognise an area.

		Third-Party Vendor Risk Management	Participants reported an area.
	VULNERABILITY	AI-Driven Attacks	Participants reported a vulnerability.
		API Security Risks	This code represents instances where participants discuss a vulnerability.
		Cloud Security Risks	Participants recognise a vulnerability.
		Data Privacy and Security Risks	Participants recognise a vulnerability.
		Identity & Access MGT weaknesses	Participants reported a vulnerability.
		Insider Threats	Participants discuss a vulnerability.
		RPA Risks	Participants reported a vulnerability.
		Supply chain Attacks	Participants reported a vulnerability.
		Third-Party Vendor Risks	Participants recognise a vulnerability.
	EXPLOIT	Compromising Third Party Vendors	Participants reported an exploit.
		Exploiting API Security Risks	Participants discuss an exploit.
		Exploiting Cloud Security Risks	Participants discuss an

			exploit.
		Exploiting Human Error	Participants reported an exploit.
		Exploiting Identity & Access MGT weaknesses	Participants recognise an exploit.
		Exploiting RPA Vulnerabilities	Participants discuss an exploit.
		Manipulating AI & ML Learning Models	Participants recognise an exploit.
		Targeting Integration Points.	Participants reported an exploit.

Table 2A: Category codebook of Theme 1.

Theme-Category Codebook of Theme 2

Research question 2	Theme	Category	Example of quotation
How can the South African digital banking industry mitigate the cybersecurity risks identified from bringing on board automation technologies for the future of work in the banking sector?	Mitigation of Cybersecurity Risks.	Organisation	"I *believe so by Implementing a Chief Information Security Office to focus on cyber resilience.*"
		Regulation	*"I believe regulatory Compliance includes Adhering to South African banking regulations (e.g., POPIA), Complying with international standards (e.g., PCI-DSS), conducting Regular security assessments and audits, implementing regulatory requirements for AI/ML, and taking Data protection and privacy measures."*

		Technology	“I*n my experience with Multi-Factor Authentication (MFA), I implement MFA across all systems and processes to provide an extra layer of security beyond just usernames and passwords.”*

Table 3A: Theme-Category codebook of Theme 2

Theme-Category Code-book of Theme 2

Theme	Category	Code	Description
Mitigation of Cybersecurity Risks.	Organisation	Continuous Improvement	Participants recognise a strategy and a new approach to mitigate cybersecurity risks.
		Employee Training and Awareness	Participants discuss a strategy and a new approach to mitigate cybersecurity risks.
		Incident Response Management	Participants reported a strategy and a new approach to mitigate cybersecurity risks.
		Third-Party Risk Management	Participants reported a strategy and a new approach to mitigate cybersecurity risks.
	Regulation	Collaboration with Regulations	Participants discuss a strategy and a new approach to mitigate cybersecurity risks.
		Compliance with Data Protection Laws	Participants discuss a strategy and a new approach to mitigate cybersecurity

			risks.
	Technology	AI-Powered Security	Participants recognise a strategy and a new approach to mitigate cybersecurity risks.
		API Security	Participants reported a strategy and a new approach to mitigate cybersecurity risks.
		Biometric Authentication	Participants reported a strategy and a new approach to mitigate cybersecurity risks.
		Blockchain Technology	Participants recognise a strategy and a new approach to mitigate cybersecurity risks.
		Cloud Computing	Participants discuss a strategy and a new approach to mitigate.
		Effective current Approaches & Tech Advancement	Participants discuss a strategy and a new approach to mitigate.
		New approaches	Participants discuss a strategy and a new

			approach to mitigate.
		Not necessary	Participants recognise a strategy and a new approach to mitigate.
		Quantum Computing and Quantum-Resistance Cryptography	Participants reported a strategy and a new approach.
		Robust Security	Participants recognise a strategy and a new approach.
		RPA Security Solution	Participants recognise a strategy and a new approach.
		Supply chain security	Participants discuss a strategy and a new approach.
		Zero-Trust Security Model	This code represents participants discussing a strategy and a new approach to mitigate cybersecurity risks.

Table 4A: Category Codebook of Theme 2.

Theme-Category Codebook of Theme 3

Research question 3	Theme	Category	Example of quotation
How does identifying cybersecurity risks associated with digital banking automation technologies in the future of work in South Africa impact the skills gap in cybersecurity professionals?	Impact of Skills Gaps on Cybersecurity Professionals.	Skills	*“I believe the new cybersecurity skill sets essential for professionals in this field are Expertise in securing AI models, understanding threats like data poisoning, and developing defences against adversarial attacks.”*
		Education	*“I believe both. Upskill current and attract new talent."*

Table 5A: Theme-Category Codebook of Theme 3

Category-Codes Codebook of Theme 3

Theme	Category	Code	Description
Impact of Skills Gaps on Cybersecurity Professionals	Skills	AI and ML Skills	Participants discuss a skill
		API Security Skills	Participants recognise a skill.
		Cloud Security Skills	Participants reported a skill.
		Data Privacy & Protection Skills	Participants reported a skill.
		DevOps and Security (DevSecOps) Skills	Participants recognise a skill.
		Identity & Access MGT Skills	Participants discuss a skill.
		New Technology Skills	Participants recognise a skill.
		RPA Skills	Participants recognise a skill.
	Education	Attract and Retain Talent	Participants discuss the impacts of skill gaps.
		Collaborate with Educational Institutions	Participants recognise the impacts of skill gaps.
		Collaborate with Industry Partners	Participants reported the impacts of skill gaps.
		Invest in Education and Training	Participants reported the impacts of skill

			gaps.
		Leverage Technology	Participants recognise the impacts of skills gaps.

Table 6A: Theme-Category Codebook of Theme 3

Table 7A below presents a comparison of theoretical expectations and findings in Proposition 1.

Theoretical Construct	**Theory (UTAUT/TOE)**	**Theoretical Expectation**	**Empirical Findings**
Perceived Risk	UTAUT (User Acceptance)	Users perceive a higher risk with increased automation technologies.	Participants reported an increase in phishing, ransomware, and social engineering attacks.
Technological Context	TOE	New automation technologies introduce both innovation and vulnerabilities.	Automation technologies tools create attack surfaces (e.g., AI-powered malware, IoT risks).
Security Vulnerability	TOE	Greater reliance on automation	Organisations struggle with

		requires stronger security controls	securing automated systems and data flows.

Table 7A: Comparison of theoretical expectations and findings in Proposition 1.

Table 8A below shows a comparison of theoretical expectations and findings in Proposition 2.

Theoretical Construct	**Theory (UTAUT/TOE)**	**Theoretical Expectation**	**Empirical Findings**
Facilitating Conditions	UTAUT	Institutional support and infrastructure aid technology adoption.	Respondents stressed the importance of regulatory frameworks and internal IT governance.
Organisational Context	TOE	Cybersecurity readiness depends on having a well-structured framework, sufficient resources, and effective policies.	Banks invest in AI monitoring, staff training, digital identity management, and other related initiatives.

Technological Readiness	TOE	Firms must adapt their cybersecurity tools in tandem with the rollout of automation technologies.	Use of SIEM, UEBA, and AI-driven anomaly detection reported.

Table 8A: Comparison of theoretical expectations and findings in Proposition 2.

Table 9A below shows a comparison of theoretical expectations and findings in Proposition 3.

Theoretical Construct	**Theory (UTAUT/TOE)**	**Theoretical Expectation**	**Empirical Findings**
Effort Expectancy	UTAUT	Users' perception of effort affects technology use and learning engagement.	Respondents note difficulty adapting to new tools due to a lack of cybersecurity training.
Human Resource Readiness	TOE	Successful tech adoption requires a skilled workforce	The skills gap in cybersecurity professionals is widening. Upskilling and training are critical.

Social Influence	UTAUT	Organisational culture influences tech acceptance and learning.	The culture of security awareness varies, affecting adaptation across banks.

Table 9A: Comparison of theoretical expectations and findings in Proposition 3.

APPENDIX B (FIGURES)

Bar chart graph of theme 1.

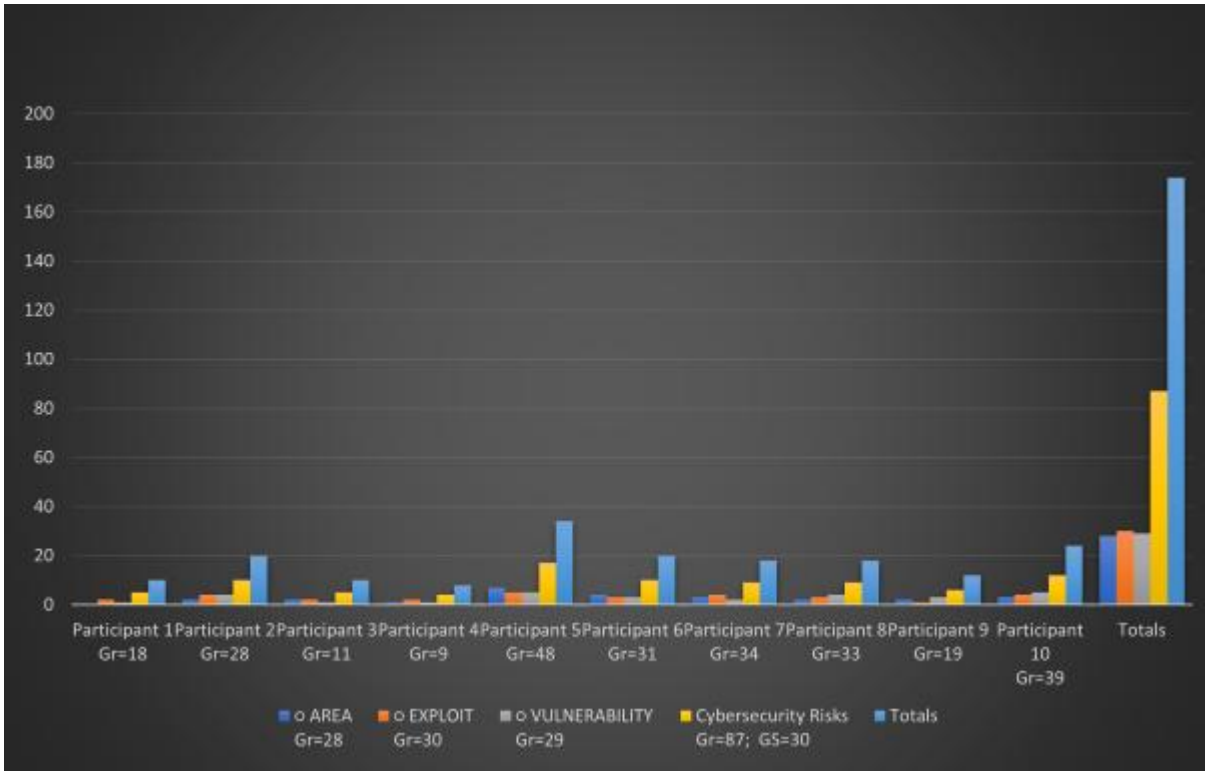


Figure 1A: Bar chart graph of Theme 1.

Word frequencies for theme 1.



Figure 2A: Word frequencies of Theme 1.

Network of Theme 1.

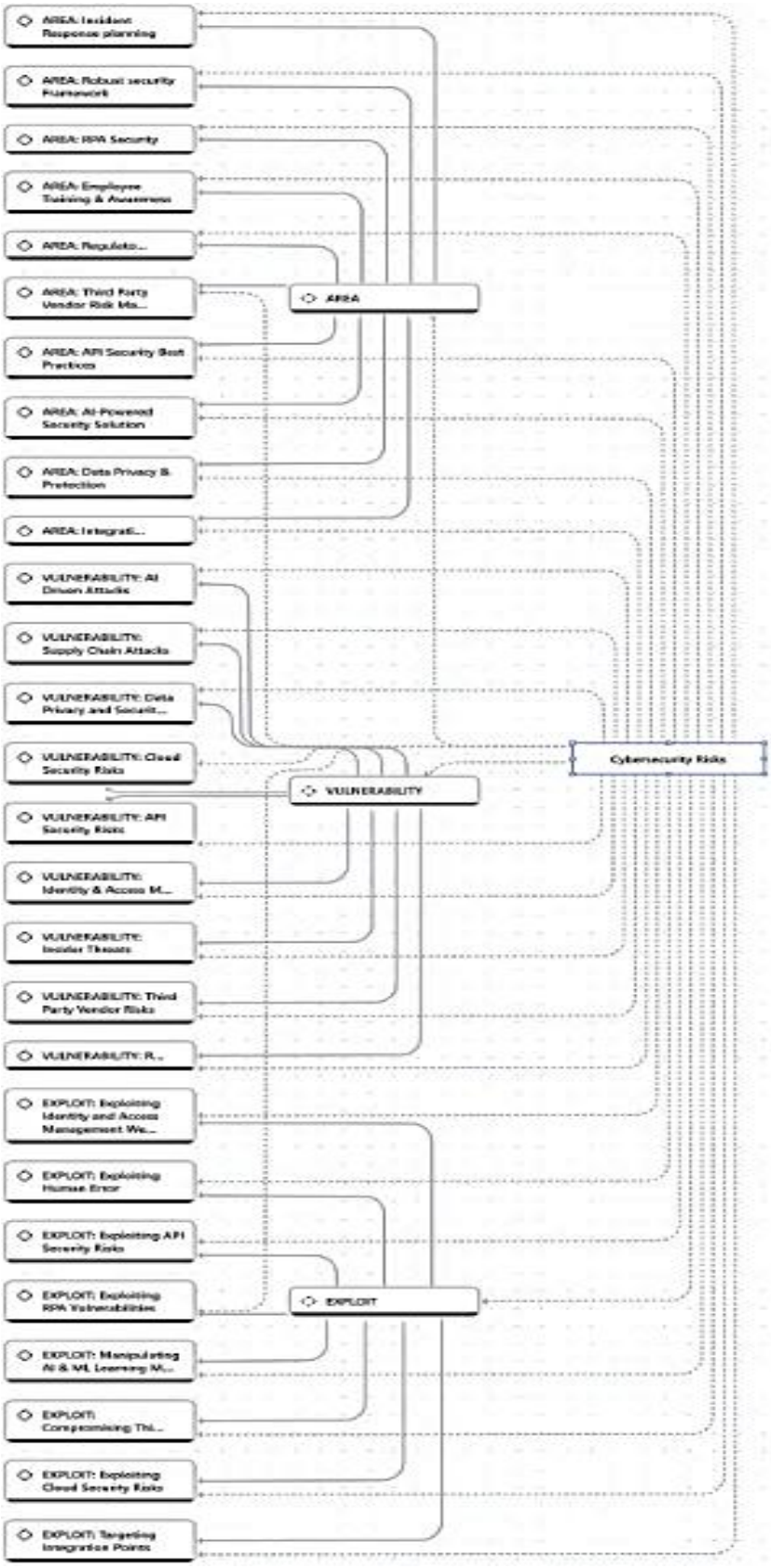


Figure 3A: Network of theme 1 with the categories and codes.

Bar chart graph of theme 2.

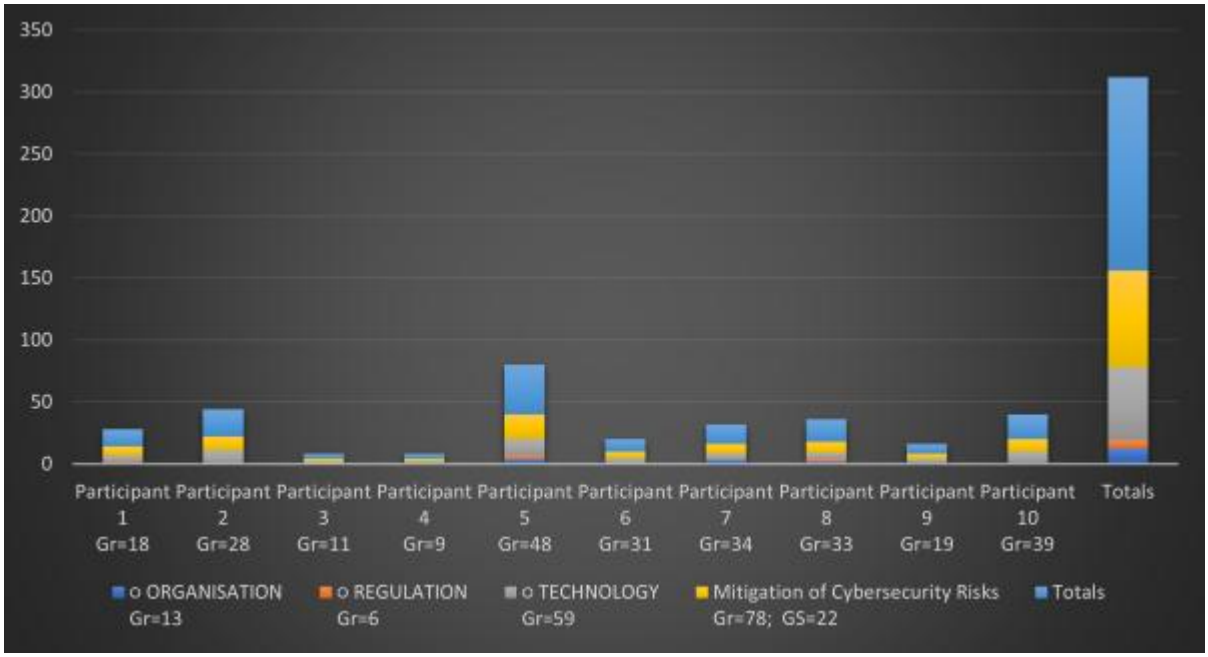


Figure 4A: Bar chart graph of Theme 2.

Word frequencies for theme 2.



Figure 5A: Word frequencies of Theme 2.

Network of theme 2 with categories and codes.

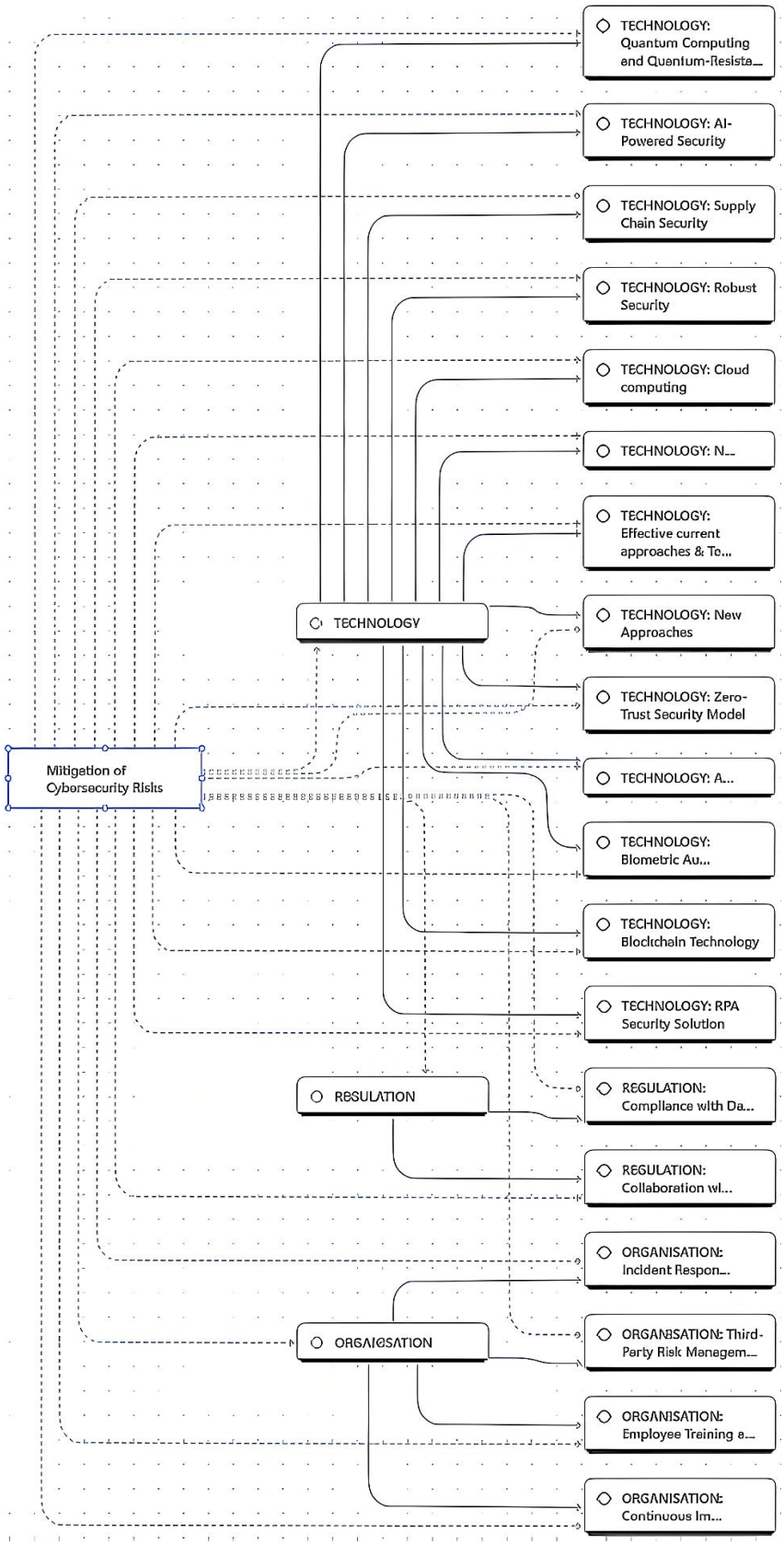


Figure 6A: Network showing theme 2 with the categories and codes.

Bar chart graph of theme 3 with the categories across ten participants.

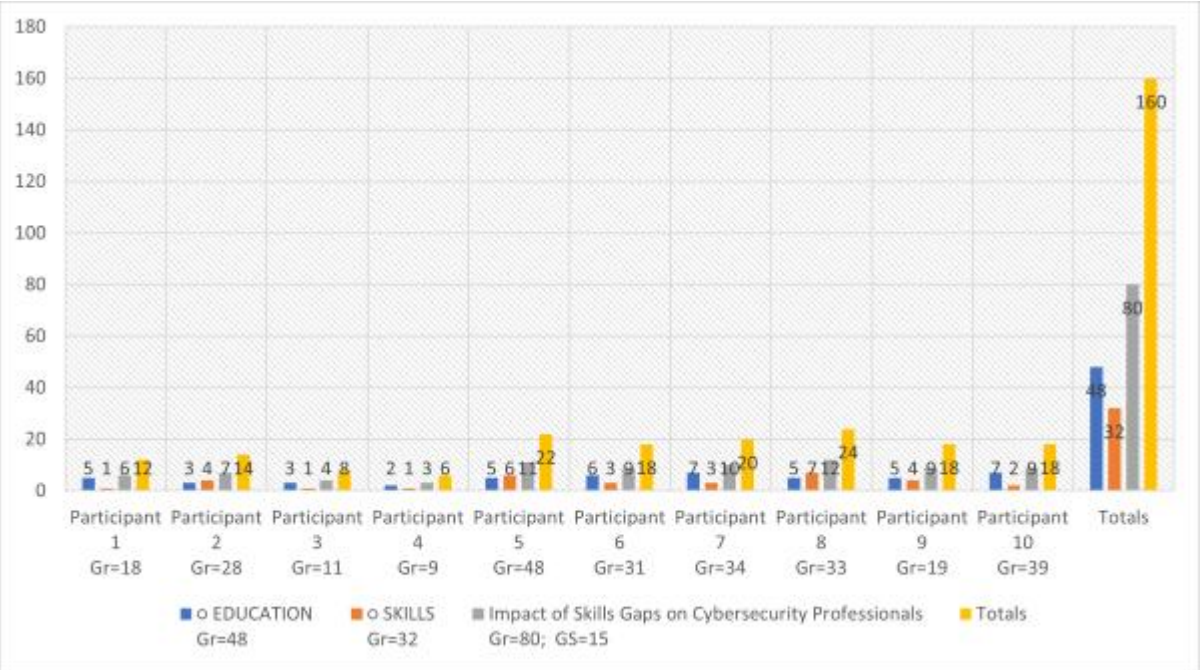


Figure 7A: Bar chart graph of Theme 3.

The figure below shows the word frequencies for theme 3.



Figure 8A: Word frequencies of Theme 3.

Network of theme 3 with the categories and codes.

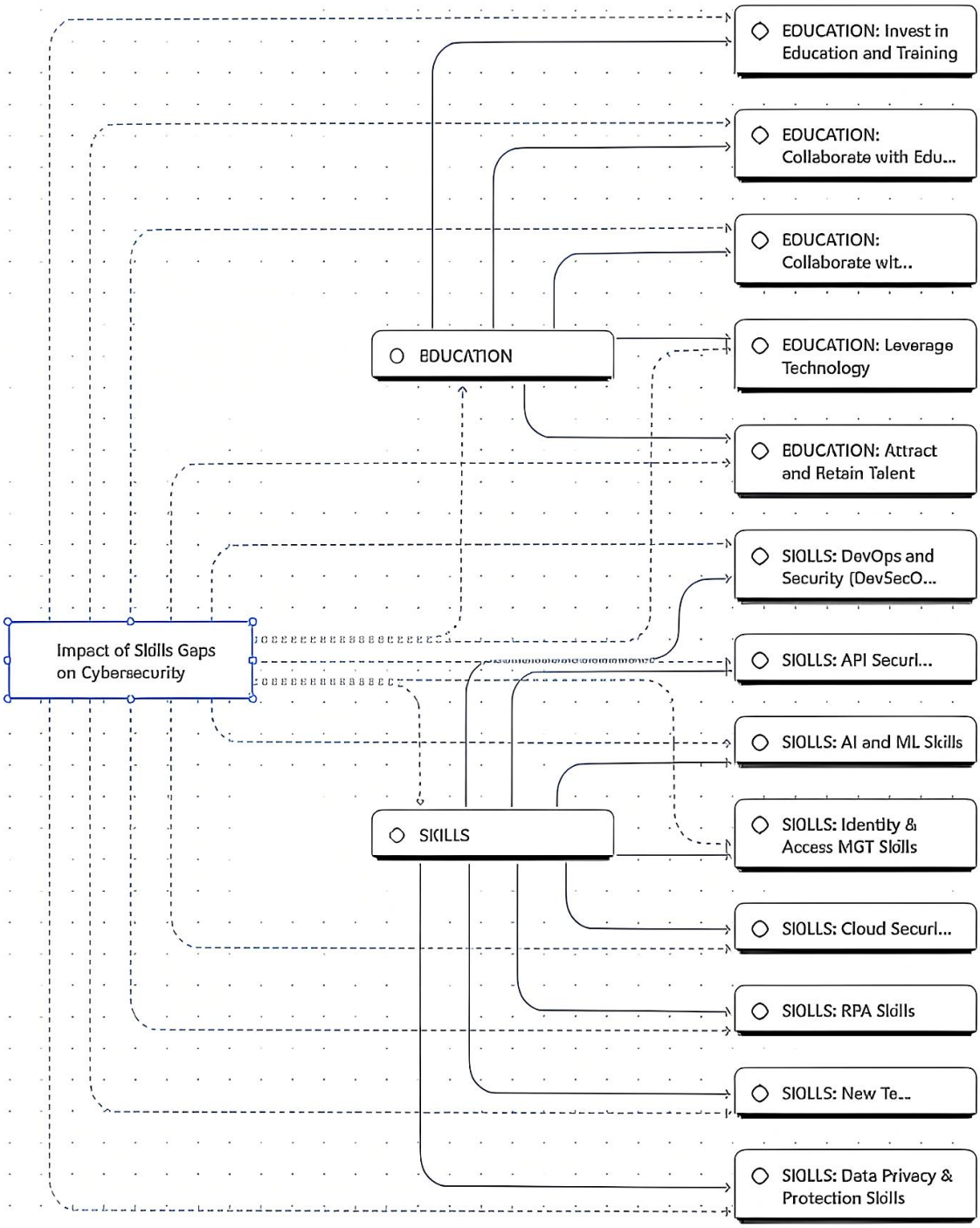


Figure 9A: Network of Theme 3 with the categories and codes.

APPENDIX C (Interview Guide)

1. With the rapid adoption of automation technologies like AI and robotics in South African banks, the urgency of understanding how these advancements could potentially increase vulnerability to cybersecurity attacks cannot be overstated. Are there specific areas within automated workflows that might be more susceptible to compromise?

2. South African banks are automating many processes, which can introduce new cybersecurity risks. Based on your experience, what specific vulnerabilities do you see emerging from automation technologies in the digital banking industry?

3. How can attackers exploit these vulnerabilities?

4. In your opinion, what specific cybersecurity measures or strategies can South African banks employ to mitigate the cybersecurity risks associated with increased automation technologies in the digital banking sector?
5. Are new approaches for mitigation needed?

6. With the rapid adoption of digital banking automation technologies in South Africa, what new cybersecurity skill sets do you see becoming essential for professionals in this field? How will these skills differ from the traditional cybersecurity skillset?

7. Given the widening skills gap anticipated with the automation technologies of digital banking processes in South Africa, what strategies can be implemented to bridge this gap?

8. Should the focus be on retraining existing professionals or attracting new talent with specialised skills?

APPENDIX D (Consent Form)

Title of Project: Cybersecurity Risks in Automation Technologies for the Future of Work in South Africa's Digital Banking Sector.

Name of Researcher: Olawunmi Adewunmi

I, ……., agree to participate in this research project.

I agree to the following:

(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I volunteer to take part in the study.	YES	NO
I agree that the interview will be audio-recorded.	YES	NO
I agree that the researcher may use direct quotations from my interview in her report.	YES	NO
I agree that my participation will remain anonymous (my name or other identifying data will not be used by the researcher in her research report.	YES	NO
I agree that other researchers may use the information I provide in my interview (depending on their own ethics clearance being obtained). Still, my name and personal information will not be used or passed on.	YES	NO

…… (signature)
…… (name of participant)
…… (date)

…… (signature)
…… (name of researcher/person seeking consent)
…… (date)

APPENDIX E (Participant Information Sheet)

Dear Sir / Madam,

My name is Olawunmi Adewunmi. I am a master's student in Digital Business at the University of Witwatersrand, Johannesburg. My supervisor is Prof. Colin Chibaya. I am conducting a research study on digital business, titled 'Cybersecurity Risks in Automation Technologies for the Future of Work in South Africa's Digital Banking Sector.'

I am inviting you to an interview session. If you decide to participate, the research study will last approximately 45 minutes for those who are interviewed. The interview will occur at your office at noon.

With your permission, I would like to audio record the interview. The data will be stored on flash drives for 20 years and then permanently deleted after this period. Only I, the researcher, will have access to the data.

The interview activity will be conducted confidentially and anonymously. When I share the research study's results, I will not include your name or any other information that could identify you. With your permission, researchers from other institutions may use the data collected from this study; however, your name and personal information will not be disclosed or shared.

You should volunteer for the research study if you choose to participate. You are not required to participate. You are free to leave the study at any moment. If you choose not to, you are not obligated to answer any questions. If you decide to participate in the research study, you won't receive any immediate advantages. You won't lose your usual rights, services, or benefits if you choose not to join. There is no cost to participate in the research study. Participation in this research study will not result in payment.

The risks associated with this research study are no greater than those encountered in everyday life. OR some of the questions may make you sad or upset. If this happens, I will stop the interview and resume it at another time.

This study will be written as a research report and will be available on the university library website. I would be happy to send you a copy of this report if you would like to receive it.

If you have any questions during or after this research study, please don't hesitate to contact me or my supervisor using the details listed below. If you have any concerns or complaints about the ethical procedures of this research study, In that case, you can contact the University Human Research Ethics Committee (Non-Medical) by telephone at +27(0) 11 717 1408 or email hrecnon-medical@wits.ac.za.

Yours sincerely,
Olawunmi Adewunmi

Researcher:
Olawunmi Adewunmi
Email: 2721656@students.wits.ac.za

Supervisor:
Prof. Colin Chibaya

Email: colin.chibaya@spu.ac.za