

https://dspace.org/

The Impact of Data Privacy Breaches on Consumer Privacy Concern and Patronage in the City of Johannesburg

Maseleme, Petronella

2023
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/40010

Maseleme, Petronella . (2023). The Impact of Data Privacy Breaches on Consumer Privacy Concern and Patronage in the City of Johannesburg [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.https://hdl.handle.net/10539/40010

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

The Impact of Data Privacy Breaches on Consumer Privacy Concern and Patronage in the City of Johannesburg

Petronella Maseleme

2380623

A research article 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 Business Administration

Johannesburg, 2023

Protocol number: WBS/BA2380623/338

(Version February 2022)

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/BA2380623/338
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below)

Project title	Data breaches and consumer privacy concerns in the City of Johannesburg
Investigator / Researcher	Miss Petronella Maseleme
Nature of Project	MBA (Research Article)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and confidentiality.
Issue Date of Certificate	25 09 2022
Expiry date	Date of submission of the project / research report
Chairperson	Prof Anthony Stacey ☎ +27 11 717 3587 +27 82 880 4531 anthony.stacey@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

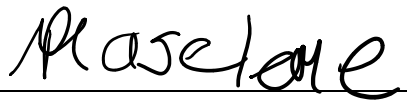
I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

Maseleme
Signature

2022/12/27
Date:

DECLARATION

I, Petronella Mahlatse Maseleme, declare that this research article is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.



(Petronella Mahlatse Maseleme)

Signed at …Johannesburg……

On the ……twenty-two……. day of …December…… 2022….

DEDICATION

This dissertation is dedicated to my mother, Thandiwe Maseleme, and to my three children, Odirile, Naledi, and Omolemo. They have been my primary source of support and inspiration throughout the completion of my Master of Business Administration (MBA). This work serves as a testament to their unwavering encouragement and belief in my abilities. I hope to demonstrate to them that there are no limits to what one can achieve with determination and hard work.

ACKNOWLEDGEMENTS

I am deeply grateful to all those who have supported and contributed to my journey throughout this study. I would like to express my gratitude to the University of the Witwatersrand Business School (WBS) for providing me with this opportunity to gain experience and learn. I would like to extend my thanks to my Lord and Saviour, Jesus Christ, for opening doors that no man could close. I am particularly grateful to my mother, Thandiwe Maseleme, who is my role model, and to my children, Odirile, Naledi, and Omolemo Maseleme, who have been a constant source of inspiration and motivation. I would also like to acknowledge my research supervisor, Dr Nakuze Chalomba, for her unwavering support and guidance throughout the completion of this work. I am truly humbled by her dedication and support. I would like to express my appreciation to my colleagues, research participants, classmates, and friends for their support. I would also like to thank Dr Bongani Munkuli for his mentorship and Dr Tafadzwa Marara for her ongoing support and language guidance. I extend my recognition and thanks to my employer, Microsoft, and to WBS, its staff, and my lecturers for providing me with a supportive platform and the tools necessary to complete this research in the discipline of a Master of Business Administration. I am forever grateful to God for his grace and mercy, and for choosing me to embark on this journey, which has been life-changing, rewarding, and humbling.

.

SUPPLEMENTARY INFORMATION

Nominated journal:	A Journal on business marketing and advertising affecting consumer patronage and trust when using digital systems and devices (Miyazaki, 2008)
Supervisor / Co-author:	Dr Nakuze Chalomba
Word count:	14 783
Supplementary files:	To Share and Protect: Using Regulatory Focus Theory to Examine the Privacy Paradox of Consumers' Social Media Engagement and Online Privacy Protection Behaviours (Mosteller & Poddar, 2017). Qualtrics Surveys were conducted to understand consumer behaviour.

ABSTRACT

The ongoing globalisation, technological advancements, and the Fourth Industrial Revolution, along with the recovery from the Covid-19 pandemic, have made digital security increasingly relevant. The shift towards conducting business and exchanging personally identifying information and personal data on digital platforms has resulted in an increased risk of cyber-attacks. The main aim of this study was to investigate data privacy breaches and their impact on consumer privacy concerns in Johannesburg. This study specifically focuses on the impact of these breaches on consumer retention within the South African context, where previous studies have not explored the phenomenon in sufficient detail. Six hypotheses were benchmarked against questions posed to 150 digital customers using cluster random sampling from employees of the City of Johannesburg and students at the University of the Witwatersrand Business School. The results were analysed using structural equation modelling, regression analysis, and analysis of variance through the use of SPSS 26 software. The findings revealed a meaningful relationship between privacy concerns, trust, assurance, regulation, and digital safety and their impact on customer retention and patronage. This study contributes to the field in three ways: conceptually, theoretically, and strategically. The results provide insights for leaders and strategists to develop multi-faceted security strategies and improve customer digital safety and online experiences.

TABLE OF CONTENTS

DECLARATION ..... **iii**

DEDICATION ..... **iv**

ACKNOWLEDGEMENTS ..... **v**

SUPPLEMENTARY INFORMATION ..... **vi**

ABSTRACT ..... **vii**

LIST OF FIGURES ..... **xii**

LIST OF TABLES ..... **xiii**

1 INTRODUCTION TO THE RESEARCH **1**

1.1 Introduction 1

1.2 Context and Background of the Study 1

1.3 Research Conceptualisation 1

1.3.1 The Research Problem Statement 2

1.3.2 The Research Purpose Statement 2

1.4 Objectives of the Study 5

1.4.1 The Research Questions 5

1.5 Hypothesis 5

1.6 Significance of the Study 6

1.7 Delimitations of the Study 6

1.7.1 Scope 6

1.7.2 Glossary of Terms 7

1.8 Assumptions 8

1.9 Significance of the Study 8

1.10 Outline of the Study 9
1.11 Summary and Conclusion of Chapter 10
2 PRELIMINARY LITERATURE REVIEW 11
2.1 Introduction 11
2.2 Background 12
2.3 Theoretical Framework 12
2.4 Study Variables 15
2.4.1 Information Privacy Concern 15
2.4.2 Unauthorised Use of Data 16
2.4.3 Compliance 17
2.4.4 Perceived Surveillance 17
2.4.5 Regulation 17
2.4.6 Trust 17
2.5 Knowledge Gaps 18
2.6 Conceptual Model 19
2.7 Hypotheses Development 20
2.7.1 Unauthorised Use of Data and Privacy Concern (Hypothesis 1) 20
2.7.2 Compliance and Privacy Concern (Hypothesis 2) 21
2.7.3 Perceived Surveillance and Privacy Concern (Hypotheses 3) 21
2.7.4 Regulation and Privacy Concern (Hypotheses 4) 22
2.7.5 Trust and Privacy Concern (Hypothesis 5) 22
2.7.6 Privacy Concern and Patronage (Hypotheses 6) 22
2.8 Conclusion 23
3 RESEARCH METHODOLOGY 24
3.1 Introduction 24

3.2 Research Strategy 24
3.2.1 Research Design 24
3.2.2 Study Area 24
3.3 Research Instruments and Data Sources 25
3.3.1 Primary Data 25
3.3.2 Online Surveys 25
3.4 Data Analysis 26
3.5 Validity and Reliability 27
3.6 Ethical Considerations 28
3.7 Anticipated Contribution of the Study 29
3.7.1 Theoretical Contribution 29
3.7.2 Weaknesses and Limitations of the Study 29
4 PRESENTATION OF RESEARCH RESULTS 31
4.1 Introduction 31
4.2 Reliability and Validity Analysis 31
4.3 Evaluating the Possible Relationship Between Privacy Concern and Unauthorised Use of Information 32
4.4 Assessment of the Potential Impact of Compliance and Perceived Regulation on Trust Perception 34
4.4.1 Descriptive Statistics – Regression Analysis 34
4.4.2 Statistical Hypothesis Testing – Linear Regression Analysis with Trust as the Dependent Variable 35
4.5 Analysing the Individual Impacts of the Perception of Surveillance on Trust and Privacy Concern Combined 36
4.5.1 Descriptive Statistics – Simple Regression Analysis 37

4.5.2 Statistical Hypothesis Testing – Simple Linear Regression Analysis with Privacy-Trust as the Dependent Variable 37
4.6 Closing of Presentation of the Findings 38
5 DISCUSSION OF RESEARCH FINDINGS 40
5.1 Introduction 40
5.2 Main Findings 40
5.2.1 Unauthorised use of data and Privacy Concern 40
5.2.2 Compliance and Privacy Concern 41
5.2.3 Perceived Surveillance and Privacy Concern 42
5.2.4 Regulation and Privacy Concern 43
5.2.5 Private and Trust 44
5.2.6 Privacy Concern and Patronage 45
5.3 Summary Findings 46
5.4 Chapter Summary 47
6 SUMMARY, LIMITATIONS, RECOMMENDATIONS, AND CONCLUSIONS 49
6.1 Summary 49
6.2 Conclusion 50
6.3 Limitations 52
6.4 Recommendations and Future Research 53
REFERENCES 57
APPENDICES 71

LIST OF FIGURES

Figure 1: Schematic representation of ISO/IEC 27001 (Adan Corporate 2013-2021) 11

Figure 2: Privacy-based Trust Violation and Repair Model 13

Figure 3: A conceptual model of the Power of Responsibilities and associated actions in identifying and curbing Privacy Concern 14

Figure 4: Schematic representation of the management of Information and Cyber Threats and Risks 16

Figure 5: Maslow's Hierarchy of Needs 18

Figure 6: Conceptual Model of the study 19

Figure 7: Schematic representation of the research methodology that will be applied 27

LIST OF TABLES

Table 1: Reliability Statistics 31

Table 2: Tests of Normality 32

Table 3: Descriptive Statistics – Spearman's Correlation Analysis 33

Table 4: Spearman Correlation Results 33

Table 5: Descriptive Statistics - Determinants of Trust 34

Table 6: Model Summary 35

Table 7: ANOVA Table 35

Table 8: Coefficients Table for Independent Variables 36

Table 9: Descriptive Statistics – Privacy-Trust and Surveillance Perception 37

Table 10: Model Summary 37

Table 11: ANOVA Table 38

Table 12: Results from the Hypotheses 46

Table 13: Proposed Timetable 85

1 INTRODUCTION TO THE RESEARCH

1.1 Introduction

The purpose of this study is to examine the impact of data privacy breaches on consumer privacy concerns and patronage in the City of Johannesburg. This introductory chapter provides the context and background of the study and outlines the research problem, research purpose, research questions, and associated research hypotheses/propositions.

1.2 Context and Background of the Study

Cybercrimes and data breaches have significantly increased in Africa, particularly in South Africa (SA), costing the economy an estimated R46 million in 2020 (Doyle Kirsten, 2019). Government departments and state-owned entities in SA, which process a large amount of personal data, including ID numbers, addresses, and credit card details, are vulnerable to cyber-attacks and breaches (Gartner, 2014). The average time for SA organisations to identify a breach is 155 days and an additional 144 days to remediate and resolve it (Dlamini & Sizwe, 2022). The financial services industry, including Experian in 2020, Nedbank in 2020, Transnet in 2021, and Absa in 2020, has been affected by these breaches. The cost of data breaches in the industrial sector is over R1,632 per compromised record (Dlamini & Sizwe, 20). The impact of these breaches extends beyond financial losses to the psychological and long-lasting impact on the SA government and the economy. In 2021, the Department of Justice and Constitutional Development was targeted and breached (Ghosal, Gallo, & Vivek, 2022), resulting in a ransomware attack that affected all electronic systems and negatively impacted ordinary citizens who were unable to access services.

Technological advancements have led to a more interconnected world, making it easier for cyber attackers to access private and sensitive data without the knowledge of the people and companies whose data is being illegally accessed.

The lack of investment in preventing cybercrimes and the ill-equipped, under-trained, and overworked South African Police Service make SA a prime target (Venter, Hein (2014). The consequences of a data breach can be significant, with SA having the third-highest number of cybercrimes reported worldwide, resulting in a loss of R2.2 billion a year (Conn, 2021). AI can be applied to software to fight cybercrime by blocking and predicting attacks, providing adequate training, using strong passwords, data encryption, firewalls, backing up data, and employing security experts.

This study will use a quantitative research method to collect data through online surveys administered to students at the University of the Witwatersrand Business School (WBS) who are employed and reside in the City of Johannesburg. The research questions will explore the impact of data privacy and AI on consumer privacy concerns and patronage.

1.3 Research Conceptualisation

The research conceptualisation of this study is discussed in this section.

1.3.1 The Research Problem Statement

The primary issue under investigation is the concern for privacy, which is impacted by several sub-problems, including the economic decline of local municipalities. In recent years, the restrictions imposed in response to the COVID-19 pandemic (Da Veiga, 2022) have further exacerbated this issue. According to a 2022 survey on cyber security breaches, the increased burden on the City of Johannesburg (COJ) as its population grows, combined with the impact of the Fourth Industrial Revolution, globalisation, high unemployment rates, and challenges in healthcare administration and safety and security, has resulted in a decreased priority being placed on cyber security and the management of data using Artificial Intelligence (Mansfield-Devine, 2022).

In July 2019, COJ experienced a network breach that resulted in unauthorised access to its critical Information and Communications Technology (ICT) systems, affecting customer-facing systems such as the billing system and all electronic services and COJ websites. This forced the city to shut down many of its services, resulting in a negative fiscal impact (Knight, 2019). Business Day (2019) reported that the city's servers and data were hacked and confidential information, such as ID numbers, addresses, and credit card details, were compromised. The hackers demanded a form of payment, threatening to upload all data to the internet if it was not received by 28 October 2019. City Power, COJ's electricity utility, was also hit by a ransomware attack in July 2019 that encrypted databases, applications, and networks (Moyo, 2019, ITWEB).

An effective cyber security strategy and plan can help COJ increase productivity, protect its websites and networks, and local municipalities, as well as efficiently mitigate the leakage of critical data. However, implementing online security and digital transformation comes with several challenges, including organisational readiness and employee resistance to change (Crittenden & Crittenden, 2008). Shina, Inga et al (2019) highlight that resistance training and management through continuous change and adoption is required to support, educate, and gain employee buy-in. Zaoui and Souissi (2020) emphasise that many businesses need to be proactive in strategy development to ensure stakeholder, management, and employee buy-in. Risk assessment programmes and initiatives are also crucial in managing and understanding organisational and employee readiness, capability, and maturity levels in implementing digital transformation strategies Zaoui & Souissi, 2020).

Organisational digital maturity, as defined by Pham Minh Hoang (2021), Murawski and Bick (2017), is the ability of organisations to mitigate risks associated with digital transformation initiatives, respond rapidly to current developments and trends, and create a competitive advantage. Improving the city's cyber security will improve its economic status and align with its mandate to secure its place as a first-world city. The costs required to maintain COJ will

decrease, allowing for allocation towards initiatives that make COJ an innovative, initiative-taking, and globally sustainable city. This study will adopt a quantitative approach, using an online survey of Wits Business School students who are also COJ residents as the primary data source, and secondary data obtained through SPSS and Microsoft Excel.

1.3.2 The Research Purpose Statement

The main aim of this study is to investigate the impact of data privacy breaches, such as unauthorised use of information and perceived surveillance, on consumer privacy concern, regulations, trust, and patronage in the COJ. These data breaches violate regulations and people's privacy, preventing them from performing basic functions, such as online payments and e-commerce functions, in the Fourth Industrial Revolution (4IR), where data is considered the new currency. The types of methods used to access confidential data have increased, and cyber criminals and hackers have become more sophisticated in their abuse of technology. In the digital age, networks and digital devices are often "illegally" accessed for financial gain at the expense of the data being used.

Data breaches occur when an individual's personal data or a company's confidential information is accessed and shared without their knowledge or consent. This unauthorised use and sharing of personal data go against regulations such as the Protection of Personal Information (POPI) Act or General Data Protection Regulation (GDPR) Act (Nel, 2017). It can also cause severe emotional and reputational damage to the victims. Data privacy refers to the ability of an individual or company to determine when, how, and with whom they would like to share their information.

1.4 Objectives of the Study

The primary objective of this study is to determine the impact of data privacy breaches on the COJ. Secondary objectives emanating from the primary objective are:

- To investigate the effects of unauthorised use of data and trust by measuring the number of incidents of unauthorised use of data through a survey.
- To investigate the effect of compliance with regulations on trust.
- To investigate the relationship between perceived surveillance and privacy concern.

1.4.1 The Research Questions

What is the relationship between unauthorised use of data and privacy concern?

How does compliance with regulations influence trust?

Does perceived surveillance positively influence privacy concern and trust?

1.5 Hypothesis

H1: There is a positive relationship between unauthorised use of data and privacy concern.

H2: There is a negative relationship between compliance and privacy concern.

H3: Perceived surveillance positively influences consumer privacy concern.

H4: Regulations have a negative influence on privacy concern.

H5: Trust has a negative influence on privacy concern.

H6: Privacy concern has a negative influence on patronage.

1.6 Significance of the Study

The outcomes of this study will provide valuable information for COJ city planners and local government authorities, enabling them to make informed decisions and take corrective action to enable COJ to become the smart city it aspires to be. This aligns with COJ's efforts to leverage its ICT and its infrastructure initiative to rebrand itself as a data-driven smart city. The study will also contribute to COJ's efforts to become an innovative and competitive city, as well as the South African government's mandate to provide transparency, convenience, safety, and a better quality of life for COJ residents and visitors.

1.7 Delimitations of the Study

1.7.1 Scope

This study focuses on the Cybercrimes and Cyber Security Act of 2020 (Hazim Gaber 2020), which was established to increase measures to prevent, detect, and remediate cybercrimes in South Africa (RSA). The study aims to provide compliance with regulations in the investigation of cybercrimes and to assist in the reporting of cybercrimes and breaches in RSA. The Act criminalises the disclosure of harmful facts and messages and enforces a cybersecurity legislative framework to address cybercrimes. The Act creates twenty new cybercrime offences and prescribes penalties for cybercrime (Government Gazette, 2021). Section 3 of the Act makes provisions for offences regarding personal information and includes proposed cybercrimes under the extension of the Electronic Communications and Transactions Act, 2002.

The following terms are defined:

Hacking: This is an action of gaining unlawful assess to digital systems and devices to create malice and commit offences. This includes confidential data like Identity Numbers and Credit Cards

Plagiarism and copyright infringements: This includes sharing and using another author Intellectual Property without their acknowledgement or permission through proper referencing and citations.

Promoting and inciting hate speech, violence, and discrimination through social media platforms like Facebook, Instagram, and Twitter.

Using dark sites to commit illegal activities.

Soliciting financial information like credit cards and banking statements without proper authorisation. This can be achieved through vishing, phishing.

The distribution of malware of digital systems and devices to create reparational damage and harm.

The global information security management standard ISO/IEC 27001 compliance process.

1.7.2 Glossary of Terms

4IR	Fourth Industrial Revolution
AI	Artificial Intelligence
COJ	City of Johannesburg
CPM	Communications Privacy Management
ECTA	Electoral Communications and Transactions Act
GDPR	Genera Data Protection Regulation

GPG	Gauteng Provincial Government
ICT	Information and Communications Technology
POPI Act	Protection of Personal Information Act
SAPS	South African Police Service

1.8 Assumptions

Assumption One: It is assumed that the variables under investigation in the study are measurable, and the instruments used to measure them are valid and dependable.

Assumption Two: For the qualitative aspects of the research, it is assumed that the survey structure accurately reflects the phenomenon and allows for data to be textually addressed to meet the research objectives. It is believed that the contributors are knowledgeable and willing to discuss the topics related to the research in order to assist with its completion.

Assumption Three: The methodology used is deemed appropriate for the problem being addressed and the goals of the study.

Assumption Four: The participants must be representative of the population and must consent to participate in the study for the research to be considered valid (Martínez-Mesa, Jeovany, et al., 2016, pp. 326-330).

Assumption Five: The study will be concluded within the given time.

1.9 Significance of the Study

The results of this study will provide valuable insight for city planners in the COJ and local government authorities, allowing them to make informed decisions and

take corrective action towards becoming a smart city. This aligns with COJ's strategic efforts to leverage its ICT and rebrand itself as a data-driven smart city, as well as its vision to become the innovation hub of Africa by 2040. This study will also support the government's mandate to provide a better quality of life for COJ residents and visitors by improving infrastructure, protecting government resources and data, and promoting transparency, convenience, safety, and better quality of life.

1.10 Outline of the Study

Chapter 1: Introduction. This chapter will provide background information on the research, define the problem statement, and outline the research objectives and questions.

Chapter 2: Literature Review. This chapter will give an in-depth analysis of the findings and theoretical framework through a review of literature and different perspectives on the relationship between privacy concerns, trust, regulation, compliance, and unauthorised use of information, and their impact on patronage.

Chapter 3: Conceptual Model and Hypothesis Development. This chapter will apply the research methodology to develop the conceptual model and hypothesis. It will also delve into the methods of data analysis.

Chapter 4: Research Design, Strategy, and Methodology. This chapter will provide a justification for the research design, strategy, and methodology, followed by the rationale for data collection and analysis. It will also include ethical considerations.

Chapter 5: Analysis of Findings. This chapter will present interpretations and a detailed analysis of the findings. The reliability, validity, and research model will be measured using statistics and illustrated using SPSS software and Microsoft Excel. Structural equation modelling will be used to evaluate the proposed research hypotheses.

Chapter 6: Evidence-based Recommendations, Limitations, and Conclusions. This chapter will provide evidence-based recommendations, limitations, and conclusions. The recommendations can be used by various stakeholders, including business owners and leaders, legislators, policymakers, residents, businesses, and their customers.

1.11 Summary and Conclusion of Chapter

This chapter has presented the purpose of the research and described its context by providing background information on the problem. The problem statement has been outlined, and the significance of the study has been discussed. The delimitation of the study has been explained in Section 1.5, while common terms used throughout the document are defined in Section 1.7.2 and assumptions are listed in Section 1.8. In conclusion, the criteria of the proposal have been outlined, addressing the issues of relevance and feasibility of the study.

2 PRELIMINARY LITERATURE REVIEW

2.1 Introduction

This literature review aims to examine the Privacy Concern as outlined in Section 1.3.1, and to evaluate the available literature on Information Security Management and compliance with ISO/IEC 27001 Standards by both consumers and organisations. The review will start by presenting a background on the significance of Privacy Concern, its resources, capabilities, and position within organisations.



Figure 1: Schematic representation of ISO/IEC 27001 (Adan Corporate 2013-2021)

The ISO/IEC 27701 standard was published in August 2019 as an extension to the ISO/IEC 27001 and ISO/IEC 27002 requirements. This was prompted by concerns that non-public information was failing to meet privacy expectations. Like most ISO requirements, continuous improvement is a principal component of ISO/IEC 27701. However, unlike other ISO requirements, there is no requirement for firms to take initiative-taking measures to comply with it.

2.2 Background

Privacy is the foundation of our freedom. This includes the lack of consumer knowledge, disclosure of cookie usage, and the role of third parties, which often leads to moments of introspection, awareness, and sufficient education for both firms and consumers (Miyazaki, 2008). Privacy concerns or beliefs do not always align with a consumer's need for privacy. Some consumers may have specific privacy beliefs about a particular website or technology, but there is considerable variation in their desire for privacy. This is similar to the distinction between locus of control, where consumers believe they have control over an event, and desire for control, where consumers are motivated to have control over the event (Sprott, Brumbaugh, & Miyazaki, 2001).

2.3 Theoretical Framework

Power Responsibility Equilibrium Model

The issues involved in ensuring an acceptable level of internet privacy are diverse. This provides several research opportunities, including how personal data is shared with third parties, collected, and stored. This brings attention to the role that legislation plays in certain countries and key industries (Petters, 2020). This is illustrated in Figure 4.

Privacy-based Trust Violation Model

The study uses two theories, the attribution theory, and the organisational justice theory, to investigate the processes and procedures that contribute to trust violation through privacy breaches and the extent of repair by company responses. Moderating effects are studied, including two types of privacy violation, hacking, and unauthorised sharing, on the trust violation and repair process. The efficacy of three response types, apology, denial, and no response, is investigated. Data was gathered using a controlled, scenario-based laboratory experiment. The results showed a significant moderating impact of violation type

on the trust violation and repair process. Apology was found to be an effective response.

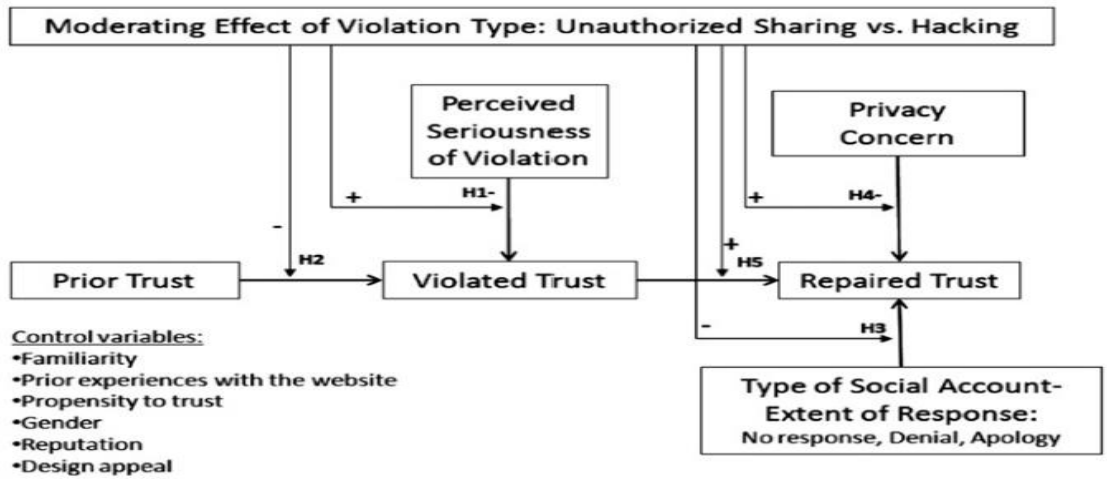


Figure 2: Privacy-based Trust Violation and Repair Model

Source: Petters (2020)

Violations of access to confidential consumer and organisational data have a significant impact on relationships and can cause irreparable reputational damage, affecting trust. Trust is commonly acknowledged as essential for any business partnership to flourish, particularly in digital environments where there is a higher level of openness and vulnerability between stakeholders. Irreparable damage, such as financial and reputational loss of revenue, can occur. Regaining trust and establishing healthy relationships between the victim and perpetrator is difficult once violated (Bansal & Zahedi, 2015, p. 71).

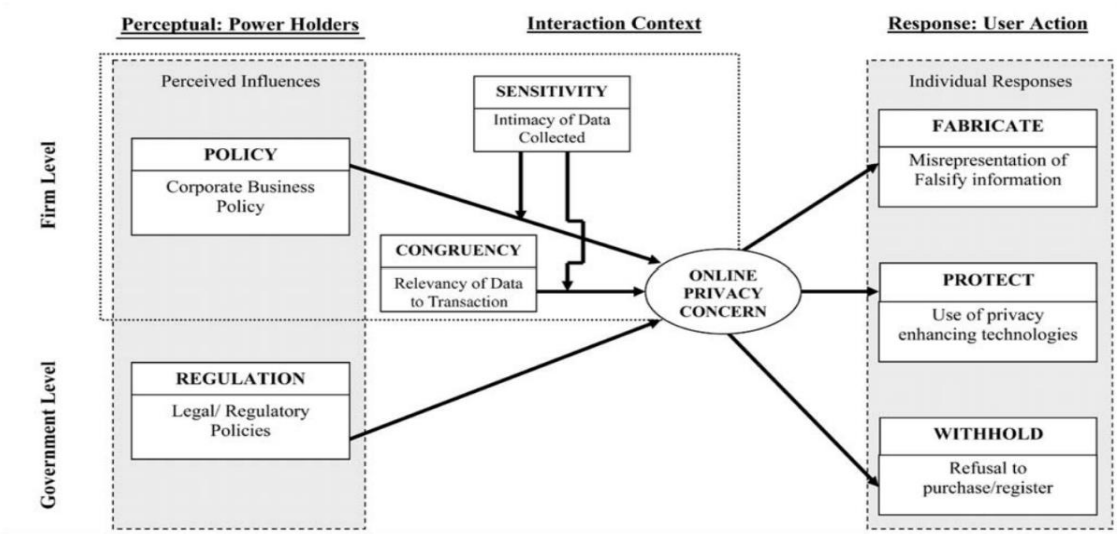


Figure 3: A conceptual model of the Power of Responsibilities and associated actions in identifying and curbing Privacy Concern

Source: Bansal and Zahedi (2015, p. 71)

The COJ needs to address the issue of Privacy Concern by considering the entire spectrum of factors that play a significant role in the matter. This includes the identification of processes, people, and systems, as well as the use of Artificial Intelligence and key stakeholders such as partners and vendors. Failure to consider one piece of the puzzle could lead to negative consequences for society and the government, resulting in a negative perception by residents and consumers regarding COJ's ability to manage and monitor confidential data, comply with regulations, and implement effective information protection policies such as the General Data Protection Regulation or the Protection of Personal Information Act. To minimise any data management risks and breaches, a holistic, end-to-end perspective needs to be adopted to assist COJ in identifying, monitoring, and managing these threats, including regulation, compliance, adherence to regulations, and building trust in the management of personal data.

2.4 Study Variables

The topic of privacy has been a matter of concern for many years, with people and organisations needing to feel safe and protected, whether personally or through the protection of physical property. Warren and Brandeis (2016) describe privacy as operating in solitude rather than the outdated need for personal privacy as common law. However, they do not delve into the issue of privacy from a business and public interest perspective. Prosser (1960) redefined privacy from four perspectives: unauthorised access into others' spaces, the disclosure of embarrassing public information about others, the inaccurate depiction of others in public spaces, and the use of organisational or consumer data without proper approval and consent.

2.4.1 Information Privacy Concern

Information privacy is a part of the broader concept of privacy and has been present before the digital age (Belanger & Crosser, 2011). However, the impact and management of information have changed with the growth of technology and the 4IR, where data has become a new currency (Belanger & Crosser, 2011; Mason, 1986). The issue of Privacy Concern is influenced by other factors such as trust, regulation, and compliance. An effective risk management system, with sufficient monitoring, processes, and systems, is crucial in managing positive customer perception and minimising the risk of data management breaches (Figure 4).

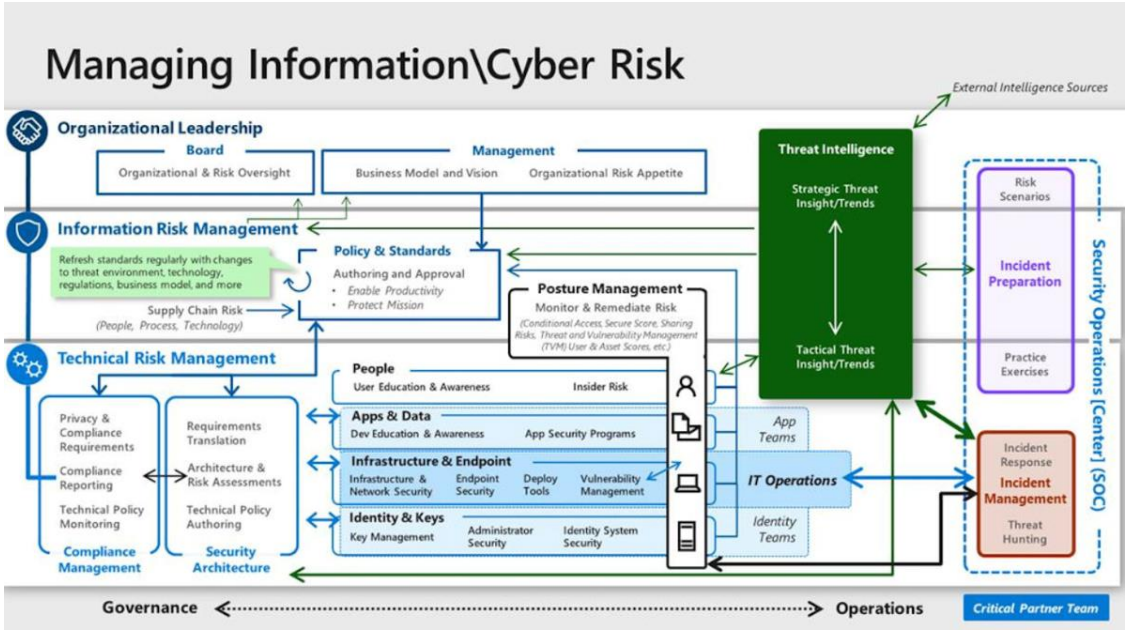


Figure 4: Schematic representation of the management of Information and Cyber Threats and Risks

Source: Ian Muscat (2019)

2.4.2 Unauthorised Use of Data

Advertisers and marketers are increasingly relying on consumer data, but firms have limited insight into the consequences of such data use and do not know how to prevent negative effects. Data management efforts may increase consumer vulnerability worries or create real vulnerability (Martin, 2017). Culnan and Williams (2009) examine the connection between individual privacy perceptions and institutional privacy assurances. They argue that by improving consumers' privacy control perceptions and reducing their risk perceptions, organisations can reduce individual privacy concerns. Leveraging the Communication Privacy Management theory (Petronio, 2002), they focus on how institutional privacy assurances, such as privacy policies and industry self-regulation (e.g., ISO/IEC 27001), can impact the reduction of individual privacy concerns.

2.4.3 Compliance

The European Union's GDPR is a leading example of data privacy laws. Since its introduction in 2018, similar measures have been introduced globally, including the California Consumer Privacy Act (CCPA) and the Brazilian Data Protection Law (LGPD) (p. 1). Depending on the location of the business and its customers, an organisation may need to comply with multiple regulatory requirements.

2.4.4 Perceived Surveillance

Smart systems and devices in homes, workplaces, and academic institutions collect a vast amount of data, raising concerns about data access and sovereignty (Shapiro & Varian, 1999, pp. 35-36). One common concern is that customers may unknowingly record their online marketing strategies through the digital devices they use.

2.4.5 Regulation

The management of the disclosure of information is the primary factor of procedural justice (Cullinan & Armstrong, 1999). This has also been referred to as "voice" in organisational justice studies (Greenberg & Folger, 1983), allowing organisations and individuals to make decisions that suit them.

2.4.6 Trust

Risk has been defined as the uncertainty of a potential negative outcome and the possibility of another party's opportunistic behaviour resulting in losses (Kyösti Pennanen,2009). Poor perceptions associated with risk can affect a person emotionally, materially, and physically (Moon, 2000).

2.5 Knowledge Gaps

In the digital era, data is as valuable as currency, and ignoring its implications could have a negative impact on people's economic and physiological well-being.

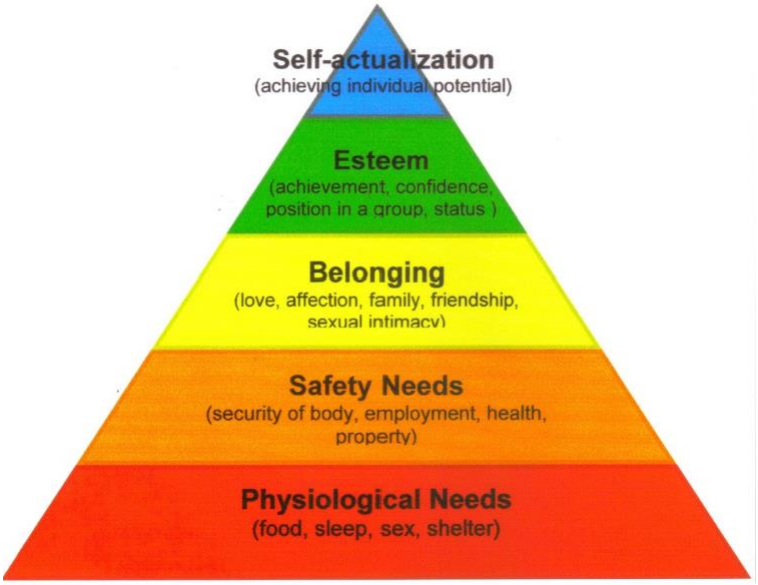


Figure 5: Maslow's Hierarchy of Needs

According to Maslow's hierarchy of needs in Figure 5, the need for privacy, safety, and security is a basic human right, just like food, water, and oxygen (ThoughtCo, 2020). The 1996 Constitution of the RSA recognises everyone is right to privacy, including privacy in their homes and online information (Leeneld, Ronald, et al. (2017). With a population of 5.7 million in 2021 (Stats SA, 2021), Johannesburg is a city with unique African character and world-class infrastructure. However, if the need for safety and security is not appropriately met, it could negatively impact the city and its inhabitants (McLeod, 2018).

2.6 Conceptual Model

The conceptual model of the study is presented in Figure 6.

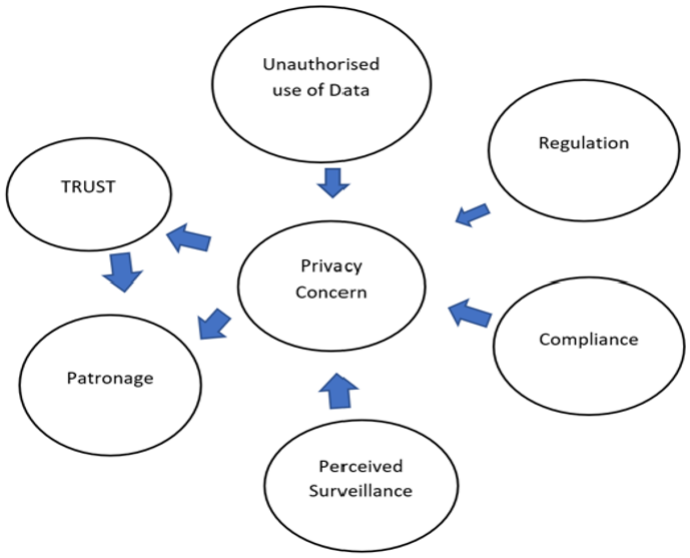


Figure 6: Conceptual Model of the study

The Conceptual Model of the study has been developed by applying two theoretical frameworks, the Power Responsibility Equilibrium Model, and the Privacy-based Trust Violation Model. These frameworks have been used to identify the six predictor variables, which are:

a) Unauthorised use of data
b) Trust
c) Patronage
d) Perceived Surveillance
e) Compliance
f) Regulation

The outcome variable in this study is Privacy Concern.

The aim of the study is to examine the relationship between these predictor variables and Privacy Concern. The Conceptual Model illustrates how Privacy Concern is directly influenced by these predictor variables, including regulation, compliance, perceived surveillance, patronage, trust, and unauthorised use of data. For example, Compliance can have a positive or negative impact on Privacy Concern, which in turn directly affects consumer trust, leading to the impact on Patronage.

2.7 Hypotheses Development

This section focuses on the development of hypotheses for the study, using the theoretical frameworks and existing literature.

For the purposes of this study, Privacy Concern refers to the access to information, which can be used for illegal purposes, resulting in harm to businesses and their customers. This includes personally identifiable information such as names, identity numbers, and date of birth. It is composed of four aspects: the attitude towards interacting with private information, the attitude towards using digital systems and technology for handling confidential information, the attitude towards regulation in managing private information, and the attitude of compliance from service providers and users of private information and systems (de Callafon, RA., FE Talke,2009).

2.7.1 Unauthorised Use of Data and Privacy Concern (Hypothesis 1)

According to the 2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) (Papaiakovou, Nika, Vergados, & IISA, 2022, pp. 1-7), the Internet of Things (IoT) applications generate vast amounts of data from various sources, including smart cities, manufacturing industries, health institutions, and governments. Due to the pervasive nature of IoT and the unlimited opportunities it provides, security and privacy have become two key concerns for users of these smart offerings. This has raised privacy threats, such

as the disclosure of confidential information to unwanted parties, leading to serious implications in various IoT applications. The growth of records technology, with its associated greater ability for surveillance, computation, storage, and retrieval, represents a real hazard to privacy, as argued by Mason (1986) and Belanger and Crosser (2011).

H1: There is a positive relationship between the unauthorised use of data and Privacy Concern.

2.7.2 Compliance and Privacy Concern (Hypothesis 2)

According to Tagarev, Todor, and George Sharkov (2019), compliance requirements that address personal information protection and security serve as a basic plan that can be followed to achieve major strengths in a secure digital security position. However, compliance has been difficult for public and private institutions, and practitioners have often been depicted as the weakest link in the security chain, failing to comply with digital transformation and online security best practices (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Vroom & Von Solms, 2004; Warkentin & Willison, 2009; Yeniman et al., 2011).

H2: There is a negative relationship between Compliance and Privacy Concern.

2.7.3 Perceived Surveillance and Privacy Concern (Hypotheses 3)

According to Dinev, Bellotto, Hart, Russo, and Serra (2008), privacy concerns impact the willingness to disclose personal information in order to engage in online activities. The perceived need for government surveillance was negatively associated with security concerns and positively associated with willingness to disclose personal information. On the other hand, concerns about government interference were positively associated with privacy concerns. Hence, perceived surveillance positively influences privacy concern.

H3: Perceived surveillance positively influences consumer Privacy Concern.

2.7.4 Regulation and Privacy Concern (Hypotheses 4)

As Cullinan and Armstrong (1999) explain, the primary factor of procedural justice is the management of the disclosure of information. This has also been referred to as the “voice” in organisational justice studies (Greenberg & Folger, 1983), allowing organisations and individuals to make decisions that suit them.

According to the Online Information Privacy Concern Instrument (OIPCI), which was used to study consumers’ expectations and experiences regarding information privacy principles in order to identify their concerns about information privacy, the study was conducted in South Africa with a representative sample of 1000 participants. Gaps were identified where consumers experienced that online organisations were not meeting their privacy expectations. This indicated that the regulatory requirements, in this case, the POPI Act, were perceived as not being met (Venter, Eloff, & Pottas, 2021). Hence, the customer surveillance positively influences consumer privacy concern.

H4: Regulation has a negative influence on Privacy Concern.

2.7.5 Trust and Privacy Concern (Hypothesis 5)

Privacy concerns have been shown to negatively impact affective trust (Ngelambong et al., 2018) and service provider trust (Ozturk et al., 2017). Privacy concerns also negatively affect people’s trust in disclosing their personal information (Bansal et al., 2015). Hence, trust negatively influences Privacy concern.

H5: Trust has a negative influence on Privacy Concern.

2.7.6 Privacy Concern and Patronage (Hypotheses 6)

According to evidence from the TRUST e-Survey, almost 92% of customers have chosen not to use retail applications due to concerns about how their personal information would be accessed and used for unintended purposes (Hakobyan,

2019). Furthermore, many consumers have ceased using digital platforms for transactions because they believed that businesses would collect too much of their personal information and misuse it (Li et al., 2019).

A great deal of effort has been devoted to defining and measuring service quality in brick-and-mortar shopping. Parasuraman et al. (1985) define service quality as the perceptions resulting from a comparison of consumer expectations with actual service performance. In order to measure service quality, Parasuraman et al. (1985, 1988) propose ten constructs (based on focus group interviews): access, communication, competence, courtesy, credibility, reliability, responsiveness, security, tangibles, and understanding/knowing customers. Hence,

H6: Privacy concern has a negative influence on patronage.

2.8 Conclusion

The previous literature review aligns with the research problem and sub-problems outlined in Section 1.4 and highlights the importance of the chosen research topic. The literature confirms the numerous factors and challenges associated with Privacy Concern and the role of the ISO/IEC 27007 standard in reducing the associated risks. It is imperative to investigate the reasons for the need to enhance the effects of cyber security, data breaches, and Privacy Concern.

3 RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the methodology that was employed in this research, including the sources of data, collection techniques, data processing, analysis, and presentation of results. The study was conducted using a quantitative research design, which will be explained in detail, including the rationale for its use. This chapter will provide a comprehensive explanation of the research methodology and the process used to collect, assemble, and evaluate the data.

3.2 Research Strategy

The research strategy is discussed in this section.

3.2.1 Research Design

This study adopted a quantitative research design. Quantitative research involves the collection and analysis of numerical data to identify patterns, numbers, and averages, evaluate causal relationships, and generalise results to wider populations (Johnson & Christensen, 2017). This approach is commonly used in natural sciences, technology studies, marketing, and economics and provides a more comprehensive understanding of the research problem than other methods. It is a more comprehensive approach (Javed, 2021).

3.2.2 Study Area

The City of Johannesburg Metropolitan Municipality is responsible for the local governance of Johannesburg in South Africa. It is divided into several branches and departments to improve service delivery and offerings for the city. IsiZulu is the most widely spoken home language, accounting for 23.4% of residents, with English as the second most spoken language at 20.1% (Stats SA, 2021).

3.3 Research Instruments and Data Sources

This section focuses on the research instruments and data sources used in this study.

3.3.1 Primary Data

Google Mapping was used to provide a mapping of the COJ Municipality to gain insight into activities within the COJ Municipality. The result was a complete GIS-generated map showing the population of the city and the number of people who have experienced data breaches. The Qualtrics survey was used to gather information which was analysed through the SPSS and Microsoft Excel on the impact of online security breaches within the Municipality.

3.3.2 Online Surveys

Online surveys were administered to conduct a behavioural analysis data set on students who are residents and WBS students who reside and work in the COJ region. The aim was to estimate and assess their perspectives and perceptions on the impact of security and privacy breaches on the city and the economic impact. The sample size was targeted at 150 participants, with seventy-five from WBS and seventy-five from COJ. The sample size was focused on people who work and reside within the City of Johannesburg, which is the economic hub of South Africa and accounts for many of all data breaches in the country (IMB & Stats SA). Written and signed consent was obtained from the COJ Municipality to conduct the study. Participants were selected through engagement with both WBS and COJ and included senior management, heads of departments, middle management, administrators, and employees.

3.4 Data Analysis

Following the collection and collation of data from primary and secondary sources, the following interpretation and analysis approaches were used:

a) Tabulation and frequency computation using descriptive statistics.

b) Development of key performance regions (KPAs).

c) Graphical illustration of statistics.

d) Multiple correlation coefficients computed using SPSS.

e) Use of Pearson's correlation approach with a confidence level of 95% and a p-value of 0.05; and

f) The F-test was applied in the analysis of variance (ANOVA).

Figure 7 illustrates the schematic representation of the research methodology that will be applied.

The Quantitative research method uses a randomized cycle of data gathering, keeping inclination from going into the information. This irregularity makes an extra benefit in the way that the data provided through this study can then be measurably applied to the population group which is under study. In spite of the fact that there is the likelihood that a socioeconomics could be forgotten about notwithstanding randomization to make blunders when the research is applied to all, the consequences of this research type make it conceivable to gather significant information quicker than other methods may require.

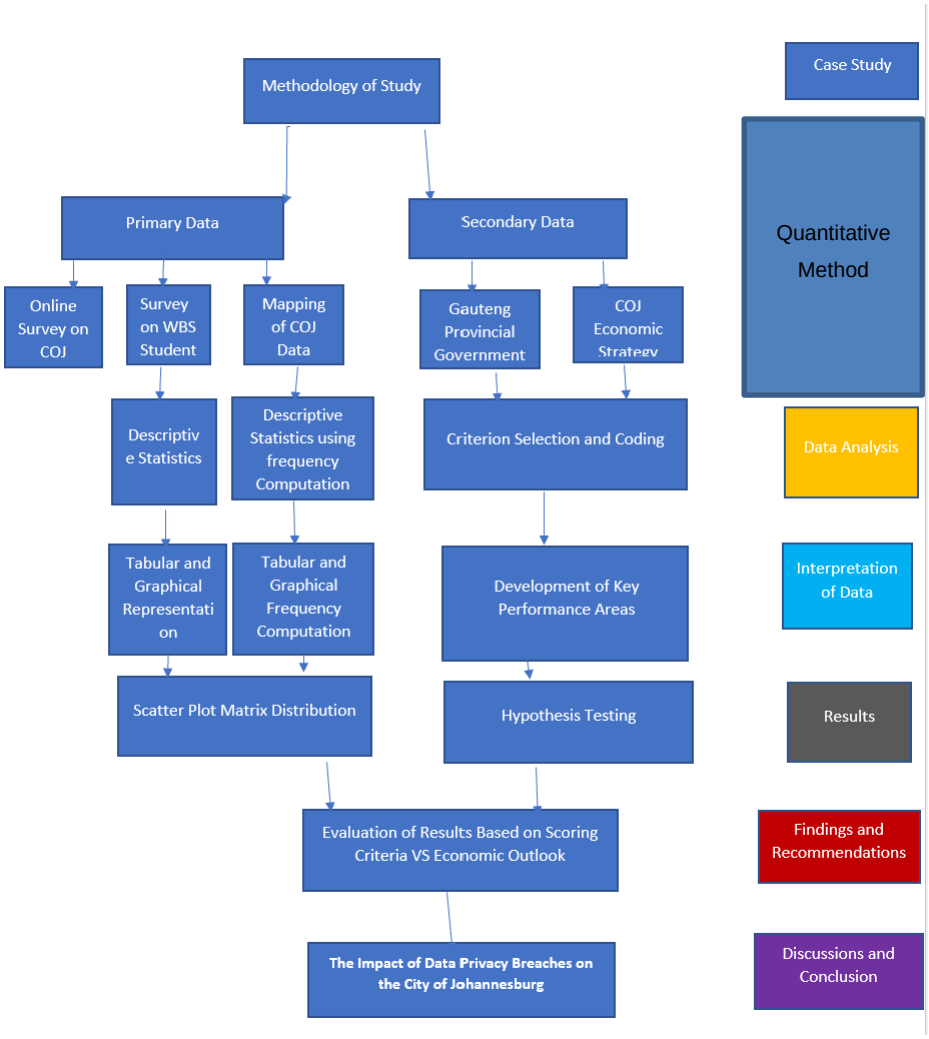


Figure 7: Schematic representation of the research methodology that will be applied. This was developed by the reasearcher.

3.5 Validity and Reliability

The validity and reliability of the measurement tool used in this research are of utmost importance. These two concepts are closely related, with validity referring to the precision of the measure and reliability referring to its consistency. To ensure the validity and reliability of the survey tool used in this study, a pilot study was conducted over a period of one week, involving individuals from both WBS and COJ.

3.6 Ethical Considerations

In conducting this research, it is the responsibility of the researcher to adhere to ethical considerations (Schindler, 2019). To ensure that the research is conducted in an ethical manner, the following processes will be observed:

(i) The researcher has obtained ethical clearance from the University's Ethics Committee.

(ii) Participants have been requested to provide consent to participate in the study.

(iii) Responses will not be linked to any individual's name, thus ensuring privacy and anonymity.

(iv) The research objectives have been articulated to ensure transparency is always maintained.

Moral contemplations in research are a set of rules that guide your exploration plans and practices. Researchers and specialists should continuously stick to a specific set of principles while gathering information from individuals or subjects.

The objectives of human research frequently incorporate real life situations and scenarios as a means of examining ways of behavioural patterns, and further developing lives in alternate ways. What you choose to research and how you direct that examination include key moral contemplations.

These contemplations work to safeguard the rights and privileges of examination subjects, improve the legitimacy and reliability of the research, and keep up with logical and scholarly trustworthiness.

3.7 Anticipated Contribution of the Study

The anticipated contribution of this study is discussed in this section.

3.7.1 Theoretical Contribution

As referred to in Chapter 2.

Expounding on the normal consequences of the study is really wise as it can assist with laying out the significance and relevance of the research. Based on the issues the researcher has identified and recognized and the proposed strategy, the study can portray what results can be anticipated from the researcher's examination and investigation.

3.7.2 Weaknesses and Limitations of the Study

This is the first study of its nature, thus making it difficult to assess the consistency and reliability of the questions as some of them were generic and not specific. This made some of the questions difficult to answer, as the respondents either did not have sufficient knowledge of the study or how to interpret some of the questions. These limitations had an impact on the validity and reliability of the data, as some respondents selected random answers to complete the questionnaire. Another limitation was the lack of control over the process and the manner in which the respondents answered the questionnaire, as the data was gathered via a survey. The tool or system was another limitation, as some respondents did not trust that their identities would be linked to their responses, due to fear of victimisation within their organisations. Despite the researcher communicating the privacy of their responses, several respondents were not comfortable with this type of study and often wondered how their data would be used. Other similar research studies conducted used controlled experiments and were conducted over a longer period. Time limitations also prevented the researcher from ensuring that the questions were suitable for receiving valid and consistent responses. A key recommendation for a researcher and the

associated institutions to conduct this type of research would be to ensure sufficient time for ethical clearances to be secured and communicated, in order to proceed with the research in a timely manner and ensure a level of trust and transparency. The researcher must also ensure that the questions are consistent and valid to avoid ambiguity. Another recommendation for this type of research would be to conduct a qualitative research method to ensure the validity of the responses.

4 PRESENTATION OF RESEARCH RESULTS

4.1 Introduction

In this chapter, the research questions will be addressed by testing the various hypotheses as identified in Section 1.2.4. First, the reliability tests will be run to construct the variables required for this analysis. Secondly, the correlation between the unauthorised use of data and the perception of privacy will be evaluated for the first research question. Thirdly, the impact of compliance and regulation on the perception of trust will be examined through regression analysis. Fourthly, the impact of surveillance on both privacy and trust will be assessed and a possible causal relationship between the stated variables will be determined. Lastly, the results of the findings will be summarised.

4.2 Reliability and Validity Analysis

The internal consistency reliability for the various variables to be used in the study was determined.

Table 1: Reliability Statistics

Scale	Cronbach's Alpha	N of Items
Privacy Concern	.744	3
Regulation Perception	.691	4
Unauthorised use of Information	.580	3
Trust Perception	.948	4
Compliance	.809	4
Patronage	.733	2
Perception of Surveillance	.786	2

A reliability analysis in the form of Cronbach's alpha was conducted to assess inter-rater reliability and obtain the statistics presented in Table 1. For the scales to be statistically reliable, a Cronbach's alpha value of at least .65 is required. As seen in the table, only the Unauthorised use of information scale did not meet this requirement ($\alpha = .580$, $n = 3$), representing a limitation in terms of data for

this study. After obtaining the reliability statistics, the means of each of the responses concerning the relevant constructs were calculated.

4.3 Evaluating the Possible Relationship Between Privacy Concern and Unauthorised Use of Information

In this section, the statistics concerning the first research question will be evaluated, in which a relationship between the privacy concern variable and unauthorised use of information will be determined. A normality test will be conducted to determine whether a Pearson's correlation analysis or its non-parametric counterpart, the Spearman's correlation analysis, should be run. The null and alternative hypotheses are identified as follows:

HO: There is no relationship between Privacy Concern and the Unauthorised use of information

H1: There is a relationship between Privacy Concern and the Unauthorised use of information.

Table 2: Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Privacy Concern Perception	.149	101	<.001	.934	101	<.001
Unauthorised Use of information	.187	101	<.001	.936	101	<.001

a. Lilliefors Significance Correction

Table 2 presents the outcome of the normality test conducted. Given that the sample size is greater than fifty, the Kolmogorov-Smirnov test will be interpreted. Results indicate that both variables yielded a statistically significant result. As a result, it can be assumed that the data is not normally distributed, and thus, the Spearman's correlation analysis can be conducted.

Table 3: Descriptive Statistics – Spearman's Correlation Analysis

	Mean	Std. Deviation	N
Privacy Concern Perception	3.6667	.96804	107
Unauthorised Use of Information	3.8350	.78687	101

The results of the Spearman's correlation analysis indicate that the mean for the variable *Unauthorised Use of Information* (M = 3.8350, SD = .78687) was highest, while *Privacy Concern* (M = 3.6667, SD = .96804) demonstrated the highest standard deviation.

Table 4: Spearman Correlation Results

			Privacy Concern Perception	Unauthorised Use of information
Spearman's rho	Privacy Concern Perception	Correlation Coefficient	1.000	.387**
		Sig. (2-tailed)	.	<.001
		N	107	101
	Unauthorised Use of information	Correlation Coefficient	.387**	1.000
		Sig. (2-tailed)	<.001	.
		N	101	101

**. Correlation is significant at the 0.01 level (2-tailed).

The results of the Spearman's Correlation Analysis indicate a moderate positive relationship between *Privacy Concern* and *Unauthorised Use of Information* ($r_s(107) = .387$, $p < .001$). Based on these findings, it is possible to reject the null hypothesis and conclude that there is a significant positive relationship between privacy concern and unauthorised use of information.

4.4 Assessment of the Potential Impact of Compliance and Perceived Regulation on Trust Perception

In the next session, a multiple linear regression was conducted to evaluate the influence of the independent variables Compliance and Perceived Regulation on Trust. The null and alternative hypotheses were formulated as follows:

HO: Compliance and Regulation has no impact or influence in terms of trust is perceived

H1: Compliance and Regulation has no impact or influence in terms of trust is perceived.

Before presenting the results of the regression analysis, it is necessary to first provide an interpretation of the descriptive statistics.

4.4.1 Descriptive Statistics – Regression Analysis

Table 5: Descriptive Statistics - Determinants of Trust

	Mean	Std. Deviation	N
Trust	3.2509	1.15748	93
Compliance	3.5771	.91702	93
Regulation perception	2.4758	.81766	93

The descriptive statistics in Table 5 indicate that Compliance had the highest mean (M = 3.5771, SD = .91702), while Trust had the highest variance (M = 3.2509, SD = 1.15748).

4.4.2 Statistical Hypothesis Testing – Linear Regression Analysis with Trust as the Dependent Variable

Table 6: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.561[a]	.314	.299	.96905	1.919

a. Predictors: (Constant), Regulation Perception, Compliance

b. Dependent Variable: Trust

The results of the multiple linear regression analysis, with Trust as the dependent variable, are presented in Table 6. The model summary indicates that the independent variables, Compliance and Regulation, explain 31.4% of the variance in the dependent variable, suggesting moderate explanatory power. It should be noted that the Durbin-Watson statistic is not interpreted, as the data collected was cross-sectional in nature.

Table 7: ANOVA Table

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	38.741	2	19.371	20.628	<.001[b]
	Residual	84.516	90	.939		
	Total	123.257	92			

a. Dependent Variable: Trust

b. Predictors: (Constant), Regulation Perception, Compliance

The results of the ANOVA test, as presented in the ANOVA table, indicate that our model satisfies the linearity assumption. This is evidenced by the significant result obtained ($R2 = .314$, $F (123.257) = 20.628$, $p < .001$). As a next step, we will examine the impact that each of the independent variables, Compliance and Regulation, has on the dependent variable, Trust.

Table 8: Coefficients Table for Independent Variables

Model		Unstandardised Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	.591	.456		1.296	.198		
	Compliance	.682	.115	.540	5.954	<.001	.926	1.080
	Regulation perception	.089	.128	.063	.696	.488	.926	1.080

a. Dependent Variable: Trust

Table 8 demonstrates the potential impact that the independent variables have on the dependent variable. It was found that Compliance was a positive predictor of Trust and was statistically significant ($\beta = .682$, $t = 3.582$, $p = .025$). This implies that, in our model, for every one unit increase in the Perception of Compliance, Trust increased on average by 68.2%. However, Regulation was found to be an insignificant predictor of Trust, as its probability value was greater than .05. Despite transforming the variable through the square root and natural log, it still did not yield meaningful results. The Variance Inflation Factor (VIF) statistics indicate that there is limited evidence to suggest the presence of multicollinearity issues.

Based on these results, it can be concluded that Compliance had an impact on how our sample perceived Trust, and the null hypothesis can be rejected.

4.5 Analysing the Individual Impacts of the Perception of Surveillance on Trust and Privacy Concern Combined

In the concluding section, we conducted another regression analysis, but with a different dependent variable – the product of Trust and Privacy Concern. The independent variable in this analysis was the Perception of Surveillance. The null and alternative hypotheses have been identified as follows:

HO: Surveillance has no influence on the newly computed Privacy-Trust variable

H1: Surveillance does have an influence on the newly computed Privacy-Trust variable.

4.5.1 Descriptive Statistics – Simple Regression Analysis

Table 9: Descriptive Statistics – Privacy-Trust and Surveillance Perception

	Mean	Std. Deviation	N
Privacy-Trust	11.7323	4.81096	88
Surveillance Perception	3.1420	.96177	88

The descriptive statistics presented in Table 9 demonstrate that Privacy-Trust had the highest mean value (M = 4.81096) and the highest variance (SD = .96177). This outcome is anticipated, as the Privacy-Trust variable is a product of two variables.

4.5.2 Statistical Hypothesis Testing – Simple Linear Regression Analysis with Privacy-Trust as the Dependent Variable

Table 10: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.124[a]	.015	.004	4.80136	1.863

a. Predictors: (Constant), Surveillance Perception
b. Dependent Variable: Privacy-Trust

The ANOVA table in Table 10 indicates that the Surveillance variable explains only a small proportion (1.5%) of the variance in the Privacy-Trust variable, implying that it has limited explanatory power in the model.

Table 11: ANOVA Table

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	31.081	1	31.081	1.348	.249[b]
	Residual	1982.564	86	23.053		
	Total	2013.645	87			

a. Dependent Variable: Privacy-Trust

b. Predictors: (Constant), Surveillance Perception

Table 11 demonstrates that the fit of the model is not adequate ($F(1,86) = 1.348$, $p = .249$). As the linearity assumption has been violated, it is not possible to proceed with the linear regression analysis. Consequently, it is concluded that the Perception of Surveillance has no impact on the combination of Privacy and Trust.

4.6 Closing of Presentation of the Findings

In this chapter, the objectives were to address the research questions and hypotheses that were established in Chapter 1. The inter-rater reliability of the scales was assessed by conducting the necessary statistics, and it was found that most of the scales were statistically dependable, except for the scale measuring Unauthorised Use of Information.

With regard to the first research question, an examination of the relationship between Privacy Concern and Unauthorised Use of Information was conducted and it was found that there was a moderate positive relationship between the two variables. The second research question focused on determining the impact of Compliance and Regulation on the perception of Trust. The results showed that only Compliance had a significant impact on Trust, while Regulation had no significant effect.

In addressing the third research question, an analysis of the impact of Surveillance on both Trust and Privacy was conducted. However, the results indicated that there was no impact as the null hypothesis could not be rejected. The findings from this chapter will be used to inform the discussion presented in the next chapter.

5 DISCUSSION OF RESEARCH FINDINGS

5.1 Introduction

This chapter aims to discuss the findings presented in Chapter 4 and to provide an analysis of the implications and probable causes related to the problem statement. The negative and detrimental implications of privacy concern on the South African economy have already been established, as demonstrated by the City of Johannesburg security breach, which cost millions of rands (Doyle Kirsten, 2019).

5.2 Main Findings

This section of the study focuses on the main findings and factors that influence the impact of data privacy breaches on consumer privacy concern and patronage in the City of Johannesburg.

5.2.1 Unauthorised use of data and Privacy Concern

$H1_0$: There is no relationship between Privacy Concern and the Unauthorised use of information.

$H1_1$: There is a positive relationship between Privacy Concern and the Unauthorised use of information.

The findings of this study indicate that there is a positive relationship between the unauthorised use of data and consumer privacy concern. This suggests a significant shift in how consumers and businesses interact with their confidential information and digital systems in the Fourth Industrial Revolution, where data is considered a new currency. To meet changing consumer needs and expectations, many organisations have had to adapt, which, along with proper governance and security regulations such as the POPI Act and GDPR, will continue to influence how organisations comply with data privacy regulations.

The right to privacy remains a fundamental human right, particularly in the digital era, where infringements can cause significant mental, financial, and reputational damage that can be difficult to correct and have long-lasting implications. The strength of the relationship between unauthorised use of data and privacy concern, as indicated by this study, is moderate (0.177), suggesting that attitude towards technology use is a predictor of employee digital readiness. Our Spearman Correlation Analysis shows that there is a significant, moderate positive relationship between Privacy Concern and Unauthorised Use of Information ($r_s(107) = .387$, $p < .001$). Based on these results, there is sufficient evidence to reject the null hypothesis and conclude that there is a significant positive relationship between privacy concern and the unauthorised use of information. These findings support previous studies on Information Privacy and Digital Systems that used various security models and frameworks. Belanger and Crosser (2011) argue that information privacy has been a part of the broader subject of privacy since before the digital age, but the impact and management of information has been transformed with the arrival of the Fourth Industrial Revolution, where data has become a new currency. This is confirmed by Mason (1986), who reasons that the growth of records technology, with its associated ability for surveillance, conversation, computation, storage, and retrieval, represents a real hazard to remaining private.

5.2.2 Compliance and Privacy Concern

$H2_0$: Compliance has a negative influence in terms of how privacy concern is perceived.

$H2_1$: Compliance has a positive influence in terms of privacy concern is perceived.

In this study, the results of Hypotheses 2 indicate a negative relationship between compliance and privacy concern. The findings indicate that compliance had a higher mean ($M = 3.5771$, Standard Deviation = .91702) and that the attitudes of respondents varied, supporting the conclusions of Cyber Security experts and

scholars (2018). This is in contrast to the findings of Antonia Handler Chayes (2009) from Cambridge University, who found that many countries comply with international regulations and agreements but may violate them when it is advantageous. This study suggests that compliance is not always based on facts or hypotheses to be tested, but rather on assumptions.

According to Cyber Security experts and scholars (2018), compliance requirements for personal information protection and security serve as a minimum standard that must be met for organisations and their clients to be considered secure. Although these requirements may be rigorous, they provide a basic plan and strategy for achieving a secure digital security posture. Compliance with digital security practices has proven to be difficult for both public and private institutions. Scholars and practitioners in the field of digital transformation have been recognised as important contributors, but they have also been identified as the weakest link in the security chain due to their tendency to neglect best practices in digital transformation and online security (Boss et al., 2009; Vroom & Von Solms, 2009). Therefore, compliance has a positive influence on privacy concern.

5.2.3 Perceived Surveillance and Privacy Concern

$H3_0$: Surveillance has a negative influence on the newly computed Privacy Concern variable.

$H3_1$: Surveillance does have a positive influence on the newly computed Privacy Concern variable.

The results of Hypothesis 3 in this study indicate that there is a positive relationship between perceived surveillance and Privacy Concern. This finding highlights the impact of digital advancements on privacy, where while they provide many benefits, they also bring along uncertainty and security risks (Kesler, G, 2009).

Organisations are collecting vast amounts of data daily, leveraging it to increase revenue and optimise profitability. Social media platforms, for instance, are used by many businesses to gather information about consumers, which is then sold to advertisers and marketers to reach their target audience (Gutierrez, S. (2014).; Vial, 2019). The methods employed by companies to collect personal data through digital platforms, networks, and technologies, such as social media monitoring, cloud computing, IoT, and digital marketing analytics, have been found to be intrusive and innovative (Sebastian et al., 2017; Vial, 2019).

Digital transformation affects organisations and employees at all levels, influencing their strategies and plans for job readiness, risk mitigation and minimisation (Steven De Haes, Caluwe, L et al., 2015; Yoo et al., 2012). As highlighted by Shapiro & Varian (1999, p. 35-36), this raises concerns about data access, ownership, and sovereignty, with online marketing strategies often recorded unknowingly by customers through the digital devices they use (Schwab, K. (2016). Hence Surveillance has a negative influence on privacy concern.

5.2.4 Regulation and Privacy Concern

$H4_0$: There is a positive relationship between Regulation and Privacy Concern

$H4_1$: There is a negative relationship between Regulation and Privacy Concern

The results of Hypothesis 4 indicate a negative relationship between Regulation and Privacy Concern. This finding supports other studies that have explored the global concern with the applicability and usability of cyber law, also known as Digital Regulation or the Law of the Web (Froomkin, 1995). This definition encompasses a set of laws that manage digital interactions on the internet using devices such as smartphones, computers, and smart devices, which have the capability of collecting data analytics about their users, such as location settings, purchasing trends, and customer behaviour and preferences. This study proposes a global solution to security, governance, and compliance.

Similarly, a study conducted by Eichensehr (2015) found that many countries agree on the need for action to prevent and monitor digital intrusions, but it also delves into the competing strategies and visions for advocating for a sovereignty-based cyber governance model that prioritises state control. The US and the UK and their allies strongly disagree with this model, arguing that cyberspace cannot be governed by individual countries alone.

According to Cyber Security Insiders and practitioners (2018), compliance requirements that address personal information protection and security serve as a basic plan and strategy to achieve a secure and highly mature digital security posture, although they can be rigorous. Another study conducted by Blythe, J., Koppel, R., & Smith, S. W. (2013) found that digital privacy and regulation should be viewed from a social contract perspective, where access to consumer data is a legally binding social contract between the data owners and those using and storing the data, which can be supported by data retention and usage policies.

5.2.5 Privacy concern and Trust

$H5_0$: Privacy Concern has a positive influence on the Trust variable.

$H5_1$: Privacy Concern has a negative influence on the Trust variable.

The findings of Hypothesis 5 in this study suggest that there exists a relationship between Privacy Concern and Trust, where Trust has a negative impact on Privacy Concern. This finding is consistent with previous studies that have indicated that Privacy Concerns have a negative effect on Trust (Ozturk et al., 2017). People are often hesitant to disclose confidential information, such as medical records, identity numbers, addresses, ages, and credit card numbers, due to the fear that this information could be used for malicious and illegal purposes, such as identity theft and financial fraud (Ngelambong et al., 2018). As a result, the relationship between Trust and Privacy Concern is adverse and negative (Bansal et al., 2015).

5.2.6 Privacy Concern and Patronage

$H6_0$: Privacy Concern has a positive influence on Patronage.

$H6_1$: Privacy Concern has a negative influence on Patronage.

The results of Hypothesis 6 in this study indicate the presence of a relationship between Privacy Concern and Patronage, where Privacy Concern has a negative impact on Patronage. This suggests that many consumers are wary and apprehensive when engaging in digital transactions due to the belief that businesses collect excessive amounts of personal information and may misuse it (Li et al., 2019).

Consistent with other studies, the TRUST e-Survey (2018) found that 92% of customers had refrained from using retail applications due to privacy concerns regarding the access and use of personal information (Hakobyan, 2019).

In this study, service quality is defined as the perception resulting from the comparison of consumer expectations and actual service performance, as proposed by Parasuraman et al. (1985, 1988). To measure service quality, ten constructs were identified through facilitating group interviews: access, communication, competence, courtesy, credibility, reliability, responsiveness, security, tangibles, and understanding/knowing customers (Parasuraman et al., 1985, 1988).

In contrast to the findings of this study, other research has taken a different approach to explore why consumers exhibit brand loyalty and what contributes to a positive customer experience. The study suggests that loyalty is positively linked to patronage, and that consumers seek convenience, high-quality services, value for money, competitive product pricing, reliability, and fast service delivery, rather than simply sticking to familiar brands and services (Forsythe & Shi, 2003). Therefore, privacy concern has a negative influence on Patronage.

5.3 Summary Findings

In this study, the six hypotheses were all supported by the findings. The first hypothesis, H1, indicated a positive relationship between Unauthorised Use of Data and Privacy. The second hypothesis, H2, indicated a negative relationship between Compliance and Privacy. The third hypothesis, H3, indicated that Perceived Surveillance positively influenced Privacy Concern. The fourth hypothesis, H4, indicated that Regulation had a negative influence on Privacy Concern. The fifth hypothesis, H5, indicated that Trust negatively influenced Privacy Concern. Finally, the sixth hypothesis, H6, indicated that Privacy Concern had a negative influence on Patronage.

Table 12 is an illustration of the results from the hypotheses.

Table 12: Results from the Hypotheses

	Hypotheses	Results
H1	There is a positive relationship between unauthorised use of data and Privacy Concern.	Significant and supported
H2	There is a negative relationship between Compliance and Privacy concern	Significant and supported
H3	Perceived surveillance positively influences consumer Privacy Concern.	Significant and supported
H4	Regulation has a negative influence on Privacy Concern	Significant and supported
H5	Trust has a negative influence on Privacy Concern	Significant and supported
H6	Privacy Concern has a negative influence on Patronage.	Significant and supported

In conclusion, the results of this study support all six hypotheses, indicating a relationship and impact between the research variables. Hypotheses H1 through H6 were supported, demonstrating the existence of a positive relationship between Unauthorised Use of Data and Privacy, a negative relationship between Compliance and Privacy, a positive influence of Perceived Surveillance on Privacy Concern, a negative influence of Regulation on Privacy Concern, a negative influence of Trust on Privacy Concern, and a negative influence of

Privacy Concern on Patronage. These findings align with previous academic literature and provide further evidence of the relationship between these variables.

5.4 Chapter Summary

This chapter presented an extensive examination of the key outcomes of the research study. The results were consistent with previous academic literature.

The research looked at the impact of protection the worries in light of multiple factors. In the first place, security concerns have been perceived as a ceaseless obstruction to online retail development (Bandara et al., 2019; Diarsenic, 2020; Martin and Murphy, 2017). Second, protection issues have been found to significantly affect buyer certainty while managing on the web exchange (Lady Or et al., 2018; Ferrell, 2017). Naturally, shoppers need to unveil specific measure of their own data in retailer's web-based stage to buy specific items or administrations. Finally, there have been calls for returning to and tending to protection issues in the contemporary setting. As featured by Smith et al. (2011), "until this point in time, numerous significant strings of data security research have grown, however these strings have not been woven together into a durable texture". While most investigations centre around protection worries at a large-scale level, the evaluation of security worries on a particular setting stays slippery and cannot be neglected (Anic et al., 2019; Bansal et al., 2015; Kayhan and Davis, 2016). Given the powerful idea of online exchange, we answer these calls by recognizing the convincing job of security worries in omnichannel retailing.

Considering previously mentioned, we make a commitment to writing in three ways. To begin with, we propose an examination model to grasp the impacts of CPCI on CE, trust, and support expectation in a comprehensive way. We view support aim as the antecedent to forming outcome in omnichannel retailing, though purchaser discernments are the vital determinants to accomplish this

momentary goal. Second, we articulate the components that support this interaction by looking at CE and trust as the consecutive go between. Third, we sustain the omnichannel retail writing by including protection worries to represent the noticed heterogeneity that would affect the connections between (I) CPCI and trust, (ii) CE and trust, and (iii) CE and support expectation.

6 SUMMARY, LIMITATIONS, RECOMMENDATIONS, AND CONCLUSIONS

6.1 Summary

The primary aim of consumer privacy concern is to safeguard individuals from the loss of privacy or privacy breaches resulting from insufficient or inadequate privacy measures. The right to privacy is recognised as a fundamental human right in numerous international treaties and conventions, including the International Covenant on Civil and Political Rights (ICCPR). This right includes the protection of personal information, enabling individuals to freely create their own personalities and identities without the fear of it being used against them for financial gain or to have leverage over organisations. Privacy breaches can result in a range of harms, including damage to reputation, emotional harm, financial setbacks, and discrimination, among others.

Organisations, both in the private and public sector, are expected to take adequate precautions to ensure the safety of personal data against breaches or unauthorised disclosure. In South Africa, the Protection of Personal Information Act (POPIA) provides rules and standards for the collection and handling of personal data. The right to privacy and protection of personal data was initially protected by common law and the Constitution, but the European Union (EU) directive that created POPIA was implemented to provide specific guidelines for organisations to follow.

Disregarding the right to privacy can also have broader societal consequences, such as a decline in public confidence and a lack of cooperation with the government, which can result in the failure of government programmes and projects.

6.2 Conclusion

The research findings indicate that compliance has a significant impact on Trust, while the impact of regulation on Trust is inconclusive. The study also found a moderately positive association between privacy concerns and unauthorised use of information. A multiple linear regression was conducted to examine the influence of compliance and regulation on individuals' perceptions of trust.

The improvement of data and correspondence innovation is developing at a high speed. Thus, the Web has become simple to get to. Thus, the quantity of Web clients has expanded immensely. In any case, most clients do not know about the fact that it is so vital to safeguard their information security on the Web, particularly as innovation is continually developing. Additionally, clients have experienced many sorts of dangers that are related with the Web, yet they may not know about them. Consequently, it is significant to evaluate the gamble related with client conduct.

It cannot be rejected that the Web means quite a bit to regular daily existence. All work, in both the general population and confidential areas, depends on IT frameworks. Consequently, frameworks should be gotten and secured. However, there are procedures and approaches that can be utilized to control clients' ways of behaving, they are not fruitful all the time. This is on the grounds that clients do not know about many gamble factors and how to safeguard themselves from or handle the gamble appropriately. Phishing is a social designing method that expects to take clients' secret data like client IDs, passwords, and banking and Mastercard details. Commonly, casualties get an email to bait them to a phony or malevolent site that requests their distinguishing data. The assault structures are changing consistently, and phishing as one of the present most serious threats.

Most openly available reports information that legislatures have, for example, name, date of birth, charge distinguishing proof number, identification number and medical care subtleties are delicate. Delicate information connected with public safety incorporate military insight, common guard, crisis plans and basic framework security. Numerous cyberattacks target outsiders to get sufficiently close to public safety information. Each nation is in danger of key cyberattacks, which is exceptionally difficult. Neither the public nor restricted areas can keep away from the danger of cyberattacks, and that implies they should track down ways of taking care of dangers appropriately and successfully.

The US Public Foundation of Principles and Innovation (NIST) gives a portrayal of safety mindfulness in NIST Exceptional Distribution (SP) 800-16, which makes sense of that bringing issues to light is not just about giving a preparation program; its primary object is to raise the consciousness of individuals to comprehend and answer cyberthreats appropriately.

Government organizations and the confidential area have devoted critical assets to guarantee data security. In any case, innovation alone is not adequate to tackle the issue as individuals are the basic objective of the cyberattack, and more often than not, this is not thought about. Subsequently, as a rule, it is basic to lay out a data security strategy to safeguard the security of data and resources by giving a functional system notwithstanding regulations, guidelines, and best practices for legitimate utilization of data innovation. In any event, when there are preparing programs set up, there are still cyber incidents; that is, preparing projects may not be adequately compelling to take care of the issue of cyberattacks.

The primary goal of any arrangement or projects intended to safeguard data ought to be to change individuals' ways of behaving bit by bit. The security

insurance methodology ought to have the option to recognize the basic ways of behaving that drive social change. For a preparation program to increment security mindfulness, individuals ought to be expected to take pretests and present tests on measure their degree of information on network safety dangers and exhibit that they know how to shield themselves from cyberattacks. However, they might know the responses when tried, they may not act likewise, in actuality. As well as preparing, there are different assets, for example, recordings, sites, and security distributions that can be utilized to increment security mindfulness. In any case, there is not a lot of exploration to assess which strategy is the best for raising network protection mindfulness. Thus, the targets of this research are to decide the best preparation strategies and to foster a model that can successfully increment network safety mindfulness.

6.3 Limitations

The study was limited by its time constraints, which was one of its key drawbacks. A longitudinal study may have been a better approach as people's attitudes can change over time, potentially affecting their responses in the study. This could also be influenced by various activities and digital engagements with different organisations. Furthermore, a more comprehensive study design, such as conducting fieldwork, might have produced more insightful findings. The use of a questionnaire was convenient, but the researcher had limited control over extraneous influences that may have affected the respondents. Additionally, the reliability measures showed unreliable results for the Cronbach alpha when it came to gauging attitudes towards risk perceptions, as there were not enough questions designed to measure such perceptions. Finally, a consultancy study using actual data from one of the businesses in the City of Johannesburg may have provided more insightful information about the real-world context.

6.4 Recommendations and Future Research

This research study focused on the Impact of Data Privacy Breaches on Consumer Privacy Concern and Patronage in the City of Johannesburg, but there are several areas for future research that could add value to this study. A mixed-method approach, incorporating both qualitative and quantitative techniques, could provide more transparent and comprehensive insights into consumer preferences and awareness levels of cyber security and privacy in the digital age, and how to protect confidential information from breaches such as phishing and malicious malware. Qualitative techniques can complement the quantitative data and provide a deeper understanding of the underlying factors. Furthermore, a focus group method would be ideal to evaluate areas of agreement and disagreement among research respondents, thereby removing any ambiguity associated with the research questions.

Finally, the study required more time, and its results were limited by the distribution of its sample, which was restricted to the City of Johannesburg and may not be representative of the South African population as a whole. It would be more accurate to assess and gauge a person's attitude and perception towards data privacy and patronage over time and across different eras and locations, rather than just one specific time and location.

Here are a few things many that can be done to minimise the impact of cyber-attacks.

Anti-virus Protection

Security awareness training is a key component of all employee training programs. There are many tools that are accessible, which most organizations and individuals can implement through a robust proactive security awareness training program. The threat from cyber criminals is not going away. Training all end users helps to minimize the threat from phishing and other social engineering attacks.

Data Protection

In your regular routine, you should try not to share actually recognizable data like your Identity Number or Credit Card Details while noting a spontaneous email, call, instant message, or text. Practicing a similar wariness at work is significant. Remember that cybercriminals can make email locations and sites that look genuine. Con artists can counterfeit guest ID data. Programmers might assume control over organization online entertainment accounts and send real messages. It could sound self-evident; however, it is significant not to release your personal or organization's information, delicate data, or licensed innovation. For example, assuming that you share an image online that shows a whiteboard or PC screen behind the scenes, you could coincidentally uncover data somebody outside the organization should not see.

Always be careful and mindful to regard the licensed innovation of different organizations. Regardless of whether it is inadvertent, sharing or utilizing the IP or proprietary innovations of different organizations could cause both the user and their organization problems.

Organizations can assist with safeguarding its representatives, clients, and information by making and appropriating business arrangements that cover themes, for example, how to annihilate information that is not required and how to report dubious messages or ransomware.

Strong password protection and authentication policies

Solid, complex passwords can help prevent cyberthieves from getting to organization data. Basic passwords can make access simple. If a cybercriminal sorts out your secret phrase, it could give them access to the organization, which

usually costs a lot of money to repair and recover the damage that could be caused. Making special, complex passwords is fundamental.

A solid secret word contains something like ten characters and incorporates numbers, images, and capital and lowercase letters. Organizations likewise ought to request that you change your passwords consistently. Changing and recalling your passwords might prove to be difficult. A password manager can assist.

Organizations may likewise require multifactor authentication when accessing sensitive data. This will add an extra layer of security by requesting that you take an additional step. e.g., providing a temporary code and is sent to the user's smart phone before signing in. This is usually a great precaution in minimising data or identity theft.

Connecting to a Safe and Secure WIFI

Office Wi-Fi's ought to be secure, encrypted, and stowed away. On the off chance that you are working from a distance, you can assist with safeguarding information by utilizing a virtual private network, assuming your organization has one. A VPN is fundamental while taking care of business beyond the workplace or on a work excursion. Public Wi-Fi can be unsafe and make your information accessible against being accessible.

However, remember, some VPNs are more secure than others. On the off chance that your organization has a VPN it trusts, ensure you know how to interface with it and use it.

Invest in Security Systems

More modest organizations could delay while thinking about the expense of putting resources into a quality security framework. That normally incorporates securities, for example, solid antivirus and malware recognition, outer hard drives that back up information, and running ordinary framework checks. In any case, making that venture early could save organizations and workers from the conceivable monetary and legitimate expenses of being penetrated.

Every one of the devices you use at work and at home ought to have the assurance of solid security programming. Your organization should give information security in the working environment, however alert your IT division or Data Security director assuming that you see whatever dubious that could show a security issue. There might be a blemish in the framework that the organization needs to patch or fix. The faster you report an issue, the better.

REFERENCES

REFERENCES

Agostino, D., Agostino, D., Arnold, V., & Bustamante, J. (2020). New development: COVID-19 as an accelerator of digital transformation in public service delivery. *Public Money & Management, 41*(1), 1-4. doi: 10.1080/09540962.2020.1764206

Albettar, M. (2019). Evaluation and assessment of cyber security based on niagara framework: A review. *Journal of Cyber Security Technology, 3*(3), 125-136. doi:10.1080/23742917.2019.1627699

Bayoumi, N. (2013). Hemodialysis Patients' Needs Priorities according to Maslow's Hierarchy and Quality of Life. *Journal of Palliative Care & Medicine, 2*(1), 106. https://doi.org/10.4172/2165-7386.1000106

Chayes, A., & Chayes, A. H. (1993). On compliance. *International Organization, 47*(2), 175-205. doi: 10.1017/s0020818300027910.

Conn, S. (2021, July 21). Gartner predicts by 2025 cyber attackers will have weaponized operational technology environments to successfully harm or kill humans. Gartner. Retrieved from www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we#:~:text=According%20to%20Gartner%2C%20security%20incidents%20in%20OT%20and.

Crittenden, V. L., & Crittenden, W. F. (2008). Building a capable organization: The eight levers of strategy implementation. *Business Horizons, 51*(4), 301-309. doi: 10.1016/j.bushor.2008.02.003

Da Veiga, A. (2022). A Study on Information Privacy Concerns and Expectations of Demographic Groups in South Africa. *Computer Law & Security Review, 47*, 105769. doi: 10.1016/j.clsr.2022.105769

Davis, D. (1997). The Constitution of the Republic of South Africa, 1993, Act 108 of 1996. *South African Journal on Human Rights, 13*(1), 1-2. https://doi.org/10.1080/02587203.1997.11834934

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2008). Internet privacy concerns and beliefs about government surveillance – an empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214-233. https://doi.org/10.1016/j.jsis.2007.09.002

Dlamini, S. (2020, August 8). Data breach at Experian, 24 million South Africans' personal information exposed. Databreaches.net. Retrieved from www.databreaches.net/data-breach-at-experian-24-million-south-africans-personal-information-exposed/.

Doyle, K. (2019, May 10). Cyber law and governance in the cybercrime age. ITWeb. Retrieved from www.itweb.co.za/content/dgp45vaGw1WMX9l8.

Eichensehr, K. E. (2014). The cyber-law of nations. *Georgetown Law Journal, 103*, 317. Retrieved from heinonline.org/HOL/LandingPage?handle=Hein.journals/glj103&div=13&id=&page=.

Eisenach, J. A. (2001). The Cyclical Behavior of the Department of Justice's Antitrust Enforcement *Activity. SSRN Electronic Journal.* doi:10.2139/ssrn.256039

Electronic Communications and Transactions Act. (2010). South African Government. Retrieved from www.gov.za/documents/electronic-communications-and-transactions-act.

Forsythe, S. M., & Shi, B. (2003, November). Consumer patronage and risk perceptions in internet shopping. *Journal of Business Research, 56*(11),

867-875. doi: 10.1016/s0148-2963(01)00273-9.

Frick, N. R. J., Loy, J. M., Bracken, C. C., & Bennett, G. G. (2021). The perceived surveillance of conversations through smart devices. *Electronic Commerce Research and Applications,* 47, 101046. doi: 10.1016/j.elerap.2021.101046

Gevers, K. (2015, October). South Africa's New Cybercrimes and Cybersecurity Bill. Data Protection Report. Retrieved from www.dataprotectionreport.com/2015/10/south-africas-new-cybercrimes-and-cybersecurity-bill/.

International Trade Administration. (2021). Impact of COVID pandemic on eCommerce. Www.trade.gov. Retrieved from www.trade.gov/impact-covid-pandemic-ecommerce.

Journal of Business Research. (2017). A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services, 73, 20-29. doi: 10.1016/j.jbusres.2016.12.002

Knight, T. (2019, July 25). POWER HIT: Cyber Crooks Try to Hold Johannesburg's City Power to Ransom. Daily Maverick. Retrieved from www.dailymaverick.co.za/article/2019-07-25-cyber-crooks-try-to-hold-johannesburgs-city-power-to-ransom/.

Kriebel, D. K., Lahti, A. C., Janusis, G. M., & Hollenbeck, J. R. (2002). Preparing for Change. *Adoption Quarterly,* *6*(2), 59-65. https://doi.org/10.1300/j145v06n02_05

Kyiv, S. (2018, September 7). Data-Driven Smart Cities: Big Data, Analytics and Security. Skelia. Retrieved from skelia.com/articles/data-driven-smart-cities-big-data-analytics-and-security/

Lwin, M. O., Wirtz, J., & Stanaland, A. J. S. (2016). The privacy dyad. *Internet Research, 26*(4), 919-941. https://doi.org/10.1108/intr-05-2014-0134

Mansfield-Devine, S. (2022). Cyber security breaches survey 2022. *Computer Fraud & Security, 2022*(4). doi:10.12968/s1361-3723(22)70568-4

Martin, K. (2017). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82*, 103-116. https://doi.org/10.1016/j.jbusres.2017.08.034

Mifdal, A. (2021, April 12). Privacy in the Twenty-First Century – ISO/IEC 27701:2019. PECB Insights. Retrieved from insights.pecb.com/privacy-twenty-first century-iso-iec-277012019/#:~:text=The%20ISO%2FIEC%2027701%20standard%20was%20published%20in%20August

Miltgen, C. L. (2009). Online consumer privacy concerns and willingness to provide personal data on the internet*. International Journal of Networking and Virtual Organizations, 6*(6), 574. https://doi.org/10.1504/ijnvo.2009.027790

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing, 27*(1), 19-33. https://doi.org/10.1509/jppm.27.1.19

Moyo, A. (2019, October 25). City of Joburg Hit by Cyber Attack. ITWeb. Retrieved from www.itweb.co.za/content/dgp45qaG8gZ7X9l8.

Moyo, A. (2021, September 23). SA Banks Caught up in Ransomware Attack on Debt Collector. ITWeb. Retrieved from www.itweb.co.za/content/rW1xLv593rlvRk6m.

Murawski, M., & Bick, M. (2017, June 5). Digital competences of the workforce - a research topic? *Business Process Management Journal, 23*(3), 721-734. doi: 10.1108/bpmj-06-2016-0126.

Nel, R. (2017, September 5). GDPR matchup: South Africa's Protection of Personal Information Act. International Association of Privacy Professionals. Retrieved from iapp.org/news/a/gdpr-matchup-south-africas-protection-of-personal-information-act/

Papaiakovou, A., Nika, C., Vergados, D. D., & IISA, (2022). E-Privacy issues in the smart city's environment. In 13th International Conference on Information, Intelligence, Systems & Applications (IISA) (pp. 1-7).

Petters, J. (2020, September 28). Data Privacy Guide: Definitions, Explanations, and Legislation. [Web log message]. Retrieved from www.varonis.com/blog/data-privacy.

Power, B. (2018). Digital transformation through SaaS multiclouds. *IEEE Cloud Computing, 5*(3), 27-30. doi:10.1109/mcc.2018.032591613

Schoonenboom, J., & Johnson, R. B. (2017). How to construct mixed methods research design. *KZfSS Kölner Zeitschrift Für Soziologie Und Sozialpsychologie, 69*(2), 107-131. Retrieved from www.ncbi.nlm.nih.gov/pmc/articles/PMC5602001/, 10.1007/s11577-017-0454-1

Shapiro, C., & Varian, H. R. (1999). *Information rules: A strategic guide to the network economy.* Boston, MA: Harvard Business School Press.

ThoughtCo. (2020, February 24). Maslow's hierarchy of needs explained. ThoughtCo. Retrieved from www.thoughtco.com/maslows-hierarchy-of-needs-4582571#:~:text=What%20Is%20Maslow%E2%80%99s%20Hierarchy%20of%20Needs%3F%201%20Physiological.

Venter, H., Eloff, J., & Pottas, D. (Eds.). (2021). Information and cyber security: 19th International Conference, ISSA 2020, Pretoria, South Africa, August 25-26, 2020, revised selected papers. Cham, Switzerland: Springer

International Publishing AG.

Wirtz, J., & Lwin, M. O. (2009). Regulatory focus on theory, trust, and privacy concern. *Journal of Service Research, 12*(2), 190-207. doi: 10.1177/1094670509335772

Writer, Staff. (2017, June 28). Counting the cost of data breaches in South Africa. Business Tech. Retrieved from businesstech.co.za/news/it-services/182293/counting-the-cost-of-data-breaches-in-south-africa/

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 2*(12), 798-824. doi: 10.17705/1jais.00281

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389-418. doi: 10.1111/j.1745-6606.2009.01146.x

“Gartner Warns of Big Data Security Problems.” *Network Security*, vol. 2014, no. 6, June 2014, p. 20, https://doi.org/10.1016/s1353-4858(14)70062-5. Accessed 17 Feb. 2023.

Dlamini, Wisdom M., et al. “Spatial Risk Assessment of an Emerging Pandemic under Data Scarcity: A Case of COVID-19 in Eswatini.” *Applied Geography*, vol. 125, Dec. 2020, p. 102358,

https://doi.org/10.1016/j.apgeog.2020.102358. Accessed 17 Feb. 2023.

Venter, Hein S. “Security Issues in the Security Cyber Supply Chain in South Africa.” *Technovation*, vol. 34, no. 7, July 2014, pp. 392–393, https://doi.org/10.1016/j.technovation.2014.02.005. Accessed 6 Sept. 2019.

Shina, Inga, et al. “Digital Transformation Outcomes in Higher Education: Pilot Study in Latvia.” *International Journal of Learning and Change*, vol. 1, no. 1, 2020, p. 1, https://doi.org/10.1504/ijlc.2020.10029097. Accessed 14 Nov. 2020.

Zaoui, Fadwa, and Nissrine Souissi. “Roadmap for Digital Transformation: A Literature Review.” *Procedia Computer Science*, vol. 175, 2020, pp. 621–628, https://doi.org/10.1016/j.procs.2020.07.090. Accessed 17 Feb. 2023.

Zaoui, Fadwa, and Nissrine Souissi. “Digital Maturity Assessment – a Case Study.” *Journal of Computer Science*, vol. 18, no. 8, 1 Aug. 2022, pp. 724–731, https://doi.org/10.3844/jcssp.2022.724.731. Accessed 22 Nov. 2022.

Gaber, Hazim. *The 2020 Cyber Security & Cyber Law Guide*. 7 Apr. 2020.

Martínez-Mesa, Jeovany. “Sampling: How to Select Participants in My Research Study?” *Anais Brasileiros de Dermatologia*, vol. 91, no. 3, June 2016, pp. 326–330, www.ncbi.nlm.nih.gov/pmc/articles/PMC4938277/, https://doi.org/10.1590/abd1806-4841.20165254.

Bansal, Gaurav, and Fatemeh Mariam Zahedi. “Trust Violation and Repair: The Information Privacy Perspective.” *Decision Support Systems*, vol. 71, Mar. 2015, pp. 62–77, https://doi.org/10.1016/j.dss.2015.01.009. Accessed 17 Feb. 2023.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review*, vol. 4, no. 5, 15 Dec. 1890, pp. 193–220, www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf, https://doi.org/10.2307/1321160.

Prosser, William L. “Privacy.” *California Law Review*, vol. 48, no. 3, Aug. 1960, p. 383, https://doi.org/10.2307/3478805. Accessed 17 Feb 2023. “Privacy.” *California Law Review*, vol. 48, no. 3, Aug. 1960, p. 383,

Mason, J. T., et al. “Letters to the Editor.” *AIChE Journal*, vol. 19, no. 6, Nov. 1973, pp. 1284–1285, https://doi.org/10.1002/aic.690190644. Accessed 17 Feb. 2023.

Muscat, Ian. “Web Vulnerabilities: Identifying Patterns and Remedies.” *Network Security*, vol. 2016, no. 2, Feb. 2016, pp. 5–10, Culnan, Mary J., and Cynthia Clark Williams. “How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches.” *MIS Quarterly*, vol. 33, no. 4, 2009, p. 673, https://doi.org/10.2307/20650322.

Petronio, Sandra. “Communication Privacy Management Theory: What Do We

Know about Family Privacy Regulation?" *Journal of Family Theory & Review*, vol. 2, no. 3, 2 Aug. 2010, pp. 175–196, https://doi.org/10.1111/j.1756-2589.2010.00052.x. Accessed 17 Feb. 2023.

Culnan, Mary J., and Pamela K. Armstrong. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." *Organization Science*, vol. 10, no. 1, Feb. 1999, pp. 104–115, https://doi.org/10.1287/orsc.10.1.104. Accessed 17 Feb. 2023.

Goyal, N K, et al. "Home Visiting for First-Time Mothers and Subsequent Pregnancy Spacing." *Journal of Perinatology*, vol. 37, no. 2, 13 Oct. 2016, pp. 144–149, https://doi.org/10.1038/jp.2016.192. Accessed 2 Sept. 2022

Kyösti Pennanen. *The Initial Stages of Consumer Trust Building in E-Commerce*. University of Vaasa, 2009.

Havlena, William J., and Wayne S. DeSarbo. "On the Measurement of Perceived Consumer Risk." *Decision Sciences*, vol. 22, no. 4, Sept. 1991, pp. 927–939, https://doi.org/10.1111/j.1540-5915.1991.tb00372.x. Accessed 17 Feb. 2023.

Moon, Hyeontae, et al. "Flooding Time Nomograph for Urban River Flood Prediction: Case Study of Dorim Stream Basin, Seoul." *Journal of Flood Risk Management*, 20 Feb. 2023, https://doi.org/10.1111/jfr3.12887. Accessed 20 Feb. 2023.

Leenes, Ronald, et al. *Data Protection and Privacy*. Bloomsbury Publishing, 28 Dec. 2017.

Mcleod, Virginia, and Clare Churly. *Atlas of Brutalist Architecture*. New York, Phaidon Press, 2018.

de Callafon, R. A., and F. E. Talke. “17th ASME Conference on Information Storage and Processing Systems at Santa Clara University, Santa Clara, CA, USA.” *Microsystem Technologies*, vol. 15, no. 10-11, 16 Sept. 2009, pp. 1479–1480, https://doi.org/10.1007/s00542-009-0922-2. Accessed 20 Feb. 2023.

Tagarev, Todor, and George Sharkov. “Multi-Stakeholder Approach to Cybersecurity and Resilience.” *Information & Security: An International Journal*, vol. 34, 2016, pp. 59–68, https://doi.org/10.11610/isij.3404. Accessed 13 May 2019.

Vroom, Cheryl, and Rossouw von Solms. “Towards Information Security Behavioural Compliance.” *Computers & Security*, vol. 23, no. 3, May 2004, pp. 191–198, https://doi.org/10.1016/j.cose.2004.01.012. Accessed 8 Feb. 2020.

Miranti, Mauren Gita, et al. “Examining Attributes Affecting Thesis Completion among Undergraduate Students.” *International Journal of Academic Research in Business and Social Sciences*, vol. 12, no. 11, 18 Nov. 2022, https://doi.org/10.6007/ijarbss/v12-i11/14756. Accessed 26 Dec. 2022.

Gupta, Chetan. “The Market’s Law of Privacy: Case Studies in Privacy and Security Adoption.” *IEEE Security & Privacy*, vol. 15, no. 3, 2017, pp. 78–83, https://doi.org/10.1109/msp.2017.57. Accessed 8 Mar. 2019.

Ali Osman Öztürk, and Mandy Herbet. *A Tasarım Mimarlık: The Architecture of Ali Osman Öztürk*. Mulgrave, Victoria, The Images Publishing Group, 2014.

Bansal and Zahedi, 2015, “Trust Violation and Repair: The Information Privacy Perspective.” *Decision Support Systems*, vol. 71, Mar. 2015, pp. 62–77, https://doi.org/10.1016/j.dss.2015.01.009. Accessed 20 Feb. 2023.

Hakobyan, V. S., et al. “Volume Expansion Mechanism of Laser-Induced Hydrodynamic Reorientation.” *Journal of Contemporary Physics (Armenian Academy of Sciences)*, vol. 56, no. 3, July 2021, pp. 196–two hundred, https://doi.org/10.3103/s1068337221030026. Accessed 12 Sept. 2022.

Li, W.-J.., Zhi, X.-Y.., & Euzeby, J. P. (2008). Proposal of Yaniellaceae fam. nov., Yaniella gen. nov. and Sinobaca gen. nov. as replacements

for the illegitimate prokaryotic names Yaniaceae Li et al. 2005, Yania Li et al. 2004, emend Li et al. 2005, and Sinococcus Li et al. 2006, respectively. *INTERNATIONAL JOURNAL of SYSTEMATIC and EVOLUTIONARY MICROBIOLOGY*, *58*(2), 525–527. https://doi.org/10.1099/ijs.0.65792-0

PARASURAMAN, D, P., D. (2012). Relevance of marketing for libraries and information managers. *International Journal of Scientific Research*, *3*(1), 209–210. https://doi.org/10.15373/22778179/jan2014/68

Johnson, R. B. (2023). Research methods: A good introduction to basic quantitative research. *Contemporary Psychology*, *47*(1), 54–56. https://doi.org/10.1037/001041

Javed, D. (2023). Research methodology: For the beginners: |Workshop by prof dr javed iqbal|. Retrieved from https://www.youtube.com/watch?v=igwqp_yIgwM.

Schindler, P. S. (2022). *Business research methods* (14th ed.). New York, Ny: Mcgraw-Hill Education.

Kessler, G. (2009). Book review: Cyber security and global information assurance: Threat analysis and response solutions. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2009.1063

Gutierrez, S. (2014). *Data scientists at work*. Berkeley, Ca Apress.

Infraestructura Vial, R. (2021). Fe de erratas. *Infraestructura Vial*, *23*(41), 31–35. https://doi.org/10.15517/iv.v23i41.45964

Steven De Haes, Caluwe, L., Huygh, T., Anant Joshi, & Springerlink (Online Service. (2020). *Governing Digital Transformation: Guidance for Corporate Board Members*. Cham: Springer International Publishing.

Schwab, K. (2016). *The fourth industrial revolution*. Geneva, Switzerland: World Economic Forum.

Eichensehr, K. (2018). Decentralized cyberattack attribution. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3369808

Blythe, J., Koppel, R., & Smith, S. W. (2013). Circumvention of security: good users do bad things. *IEEE Security & Privacy*, *11*(5), 80–83. https://doi.org/10.1109/msp.2013.110

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance. *Journal of Global Information Management*, *14*(4), 57–93. https://doi.org/10.4018/jgim.2006100103

Venter, H. S., & Eloff, J. H. P. (2003). Assessment of vulnerability scanners. *Network Security*, *2003*(2), 11–16. https://doi.org/10.1016/s1353-4858(03)00211-3

APPENDICES

APPENDIX A: CONSISTENCY MATRIX

Problem or scope of project stated here					
Sub-problem	Literature Review	Hypotheses or propositions or questions	Source of data	Type of data	Analysis
How does cyber security breaches influence consumer Privacy and Patronage in the City of Johannesburg	Miyazaki, Anthony D. “Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage.” *Journal of Public Policy & Marketing*, vol. 27, no. 1, Apr. 2008, pp. 19-33, 10.1509/jppm.27.1.19.	H5 Trust has a negative influence on Privacy Concern. H6: Privacy concern has a negative influence on patronage.	Observational data collected using an online survey.	Nominal Data	Structural Equation Modelling Analysis

Problem or scope of project stated here					
Sub-problem	Literature Review	Hypotheses or propositions or questions	Source of data	Type of data	Analysis
Does Regulation and Compliance affect consumer digital readiness in the COJ Industry?	Petters, Jeff. “Data Privacy Guide: Definitions, Explanations and Legislation.” Www.varonis.com, 28 Sept.2020, www.varonis.com/blog/data-privacy. Accessed 11 June 2022.	H2: There is a negative relationship between compliance and Privacy Concern. H3: Perceived surveillance positively influence consumer Privacy Concern.	Observational data collected using an online survey.	Nominal Data	Structural Equation Modelling Analysis

Problem or scope of project stated here					
Sub-problem	Literature Review	Hypotheses or propositions or questions	Source of data	Type of data	Analysis
How does the unauthorised use and access of data affect privacy within the COJ?	YOUN, SEOUNMI. "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviours among Young Adolescents." *Journal of Consumer Affairs*, vol. 43, no. 3, Sept. 2009, pp. 389-418, 10.1111/j.1745-6606.2009.01146.x.	H1. There is a positive relationship between unauthorised use of data and Privacy Concern. H4 Regulation has a negative influence on Privacy Concern.	Observational data collected using an online survey and questionnaire.	Nominal Data	Structural Equation Modelling Analysis

APPENDIX B: INVITATION LETTER / PARTICIPATION INFORMATION SHEET

Good day,

My name is Petronella Maseleme, and I am studying master's in business administration from Wits Business School. As part of my studies, I must undertake a research project and the title of the research project is as follows: The Impact of Data Privacy Breaches on Consumer Privacy Concern in the City on Johannesburg

The main aim of this study is to investigate Data Privacy Breaches such as unauthorised use of information and perceived surveillance on consumer privacy concern in the city of Johannesburg. The primary objective of this study is to determine the impact of data privacy breaches on the City of Johannesburg.

I would like to invite you to take part in answering an anonymous and confidential survey. This activity will involve answering questions based on whether you agree with the statement or not and will take around ten minutes of your time. All the data collected in the study will not be shared with third parties, the questionnaire and final report will be used for academic purposes, and only aggregate or the combined results will be reported in the final report. Your participation will be valuable to my studies and will assist towards investigating and providing a solution for the current challenges faced using digital technology and minimising information breaches.

You will not receive any direct benefits from participating in this research, and there are no disadvantages or penalties for not participating. You may withdraw at any time or not answer any question if you do not want to. The survey will be

completely confidential and anonymous. Please note that by submitting the completed questionnaire your agreement to participation in this research is assumed. Thank you for taking the time to read this information.

APPENDIX C: PARTICIPANT CONSENT FORM

Participant Consent Form

I would hereby like to give consent to take part in the research on the Exploratory Study into the impact of Data Privacy Breaches on Consumer Privacy Concern and Patronage in the City of Johannesburg.

☐ I have read the Information Sheet, have asked questions about the study, and have satisfactory answers to my questions.

☐ I understand that this study has been reviewed by WBS research department and received ethical clearance and approval.

☐ I understand that participation is voluntary and that I am free to withdraw myself or any data during the first six (six) months of this study from January 2022, with a reasonable explanation.

☐ I understand that I should have the necessary information, knowledge, and perceptions on consumer's data privacy needs

☐ I understand that my identity will remain anonymous and that my personal information will not be shared.

☐ I understand that the research data, which will be anonymous.

☐ I understand how the study will be written up and published.

☐ I understand that I may seek further information on the study from the researcher: Petronella Maseleme (0732602615)

I have initialled the above boxes myself and I agree to take part in the study. All information obtained will be treated in strictest confidence.

_____ _____

Participant Signature

_____

Date

Please return to 2380623@students.wits.ac.za

APPENDIX D: ONLINE SURVEY\QUESTIONNAIRE

SECTION A: DEMOGRAPHICS

This section is about background information. Please tick (X) appropriate answer:

A1: Gender

Male		Female	

A2: Age

18 - 29 years	
30 - 39 years	
40 - 49 years	
50 - 59 years	
60 or more years	

A3: Level of Education

Grade 12/Matric	
Certificate	

Bachelor’s Degree	
Honours/Postgraduate Diploma	
Masters	
PhD	

A4: INDUSTRY

Commercial (Sales and marketing)	
Medical Affairs	
Regulatory	
Research and Development	
Manufacturing	
Other	

Section B:

Regulation

Please indicate to what extent do you Agree/ Disagree with the statements below regarding REGULATION in your Organization

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
The existing laws in my country are sufficient to protect company and consumers' online privacy.	○	○	○	○	○
International laws to protect personal information of individuals on the Internet are stringent	○	○	○	○	○
The government is doing enough to ensure that its citizens are protected against online privacy breaches	○	○	○	○	○

Privacy Concern

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
PC1	I have a concern that my confidential information has been collected and stored by organisations without my knowledge or consent					
PC2	I have a concern that					

	organisations and individuals have collected my confidential information is accessible and used without my knowledge. (e.g., hacking and fishing)					
PC3	I am concerned that confidential information collected by my organisation is accessible by colleagues and peers is used without my knowledge and consent (e.g., emails can be used for illegal or promotional purposes)					
PC 4	I am concerned that my organisation shares the					

	classified information it collects with unauthorised external individuals or companies (e.g., this information and data could be sold to other organisations without my knowledge)					

Unauthorised use of information

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
UUI1	Organisations should never use the information for any purpose other than that for which it was intended.					
UUI2	Organisations should never					

	sell their customer's personal information					
UUI3	Organisations should never share their customer's personal data unless the owners of the information granted consent and authorisation					
UUI4	Organisations should always disclose when the personal information has been accessed illegally by others					

TRUST

Q8

Please indicate to what extent do you Agree/ Disagree with the statements below regarding TRUST within your Organization

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
I have trust in my organization and the government	○	○	○	○	○
My organisation is Trustworthy	○	○	○	○	○
I have confidence in the Organization's conduct	○	○	○	○	○
My organisation is reliable	○	○	○	○	○

COMPLIANCE

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
The Organization would not use personal data of customers for purposes other than those initially stated on their sites and browsers.	○	○	○	○	○
The Organization would not share your personal information with external parties without the consent, knowledge and approval individuals who own the information.	○	○	○	○	○
Databases that contain personal data are protected from unauthorized access regardless of costs	○	○	○	○	○

PATRONAGE

Q10.

Please indicate to what extent do you Agree/ Disagree with the statements below regarding PATRONAGE within your Organization

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	AGREE
My personal information is updated most of the time	○	○	○	○	○
I inform my organization regarding changes in my personal information	○	○	○	○	○
I generally volunteer additional information to my organization	○	○	○	○	○

SURVEILLANCE

Q11

Please indicate to what extent do you Agree/ Disagree with the statements below regarding SURVEILLANCE within your Organization

- ○ I think online Surveillance is a good deterrent of criminal behaviour - I like it
- ○ Online Surveillance is a privacy violation - i don't like it

APPENDIX E: METHODOLOGY

PROPOSED TIMETABLE

Table 13: Proposed Timetable

	INPUT	**DESCRIPTION**	**DURATION**	**TARGET DATE**	**OUTPUT**
s/n	**A.**	**B.**	**C.**	**D.**	**E.**
1.	Supervisor Allocation	1.1 Introductions of establish rapport and Rhythm of Engagement with Supervisor.	24 March-June 01	April 8 2022	Rapport with supervisor
2.	Submission of proposal	1.1 Proposal Planning and Formulation. 1.2 Proposal Submission	June 01-June 14	June 15 2022	Proposal submission
3.	Proposal Defence	1.1 Proposal defence to the WBS ARP panel	June 15 - June 17, 2022,	20 June 22	Approval of proposal

4.	Introduction	1.1 Background 1.2 Research problem 1.3 Research Aim and Purpose 1.4 Research objectives 1.5 Hypotheses 1.6 Rationale 1.7 Study area 1.8 Scope of the study 1.9 Significance of the study 1.10 Target audience 1.11 Chapter Outline 1.12 Chapter Summary	June 20, 2022	25 July 2022	Submission of Chapter 1: Introduction

5.	Literature review	2.1 Introduction 2.2 Global context 2.3 Regional context 2.4 Local context 2.5 Legislative requirement 2.6 Paradigm context of the study 2.7 Conceptual framework of the study 2.8 Key Knowledge gaps 2.9 Summary of chapter	July 20 - August 15 2022	Aug 15 2022	Submission of Chapter 2: Literature Review

6.	Methodology	3.1 Introduction 3.2 Materials and methods 3.2.1 Research design 3.2.2 Population 3.2.3 Data sources 3.2.4 Instruments and data collection 3.3 Summary of chapter	7 Aug-15 Aug 22	16 Aug 22	Submission of Chapter 3: Methodology
7.	Data Collection	4.1 Introduction 4.2 Collection of data 4.3 Summary of chapter	16 Oct 22	16 Oct 22	Submission of Chapter 4: Data collection
8.	Data Analysis	5.1 Chapter Introduction	16 Oct-15 Nov 22	15 Nov 22	Submission of

		5.2 Descriptive statistics 5.3 Regression outputs 5.4 Correlation 5.5 ANOVA 5.6 Standard coefficient 5.7 Key knowledge gaps 5.8 Summary of chapter			Chapter 5: Data Analysis
9.	Presentation of Results, Recommendation, and conclusion	6.1 Chapter Introduction 6.2 Results and Discussions 6.3 Recommendations 6.4 Contribution to the study 6.4.1 Methods 6.4.2 Policy	10 Nov-10 Dec 22	14 Dec 22	Submission of Chapter 6 Finalisation and complete

		6.4.3 Key findings 6.4.4 Knowledge gaps addressed. 6.4.5 Limitations of the study 6.5.6 Goals and principles of the study 6.5 Recommendations 6.6 Conclusion			
10.	Submission for Editing		14 Jan 23		Professional Editing
11.	Preparation and Submission to Faculty		15 Feb 23		Complete paper
12.	Submission of Thesis to Faculty				