

https://dspace.org/

Assessing cybersecurity vulnerabilities in the disposal of ewaste in South African public & private institutions

Khumalo, Dimitri

2022

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/34667

Khumalo, Dimitri. (2021). Assessing cybersecurity vulnerabilities in the disposal of ewaste in South African public & private institutions [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.https://https://hdl.handle.net/10539/34667

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

Assessing cybersecurity vulnerabilities in the disposal of e-waste in South African public & private institutions

Dimitri Khumalo

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

Johannesburg, 2021

ABSTRACT

Over the years there have been numerous studies conducted, focusing on the various facets of waste electronic and electrical equipment, also termed electronic waste or e-waste, and the impact it has on the environment. However, little attention has been placed on the management of personal data during the disposal phases of e-waste and the inherent ramifications it poses if this data were retrieved.

This study sought to assess the vulnerabilities to which organisations are exposed, specifically financial and government institutions, by interrogating the management policies, processes, and procedures for stored data when disposing of e-waste at the end of the asset life cycle.

A qualitative research method, through semi-structured interviews was conducted. The population selected were very senior individuals, selected based on the specific roles and experiences they fulfilled within the financial services sector, various government institutions, and e-waste recycling companies.

From the findings, it emerged that there were growing concerns around the effective policy regulations put in place to manage the disposal practices of e-waste and that of personal identifiable and sensitive data of individuals. This has driven a need for policies and robust mechanisms to be instituted to try and minimise the overall impact these vulnerabilities could pose to the environment and the entire value chain, at that juncture where electronic devices have reached their EOL and are now being disposed of.

The results demonstrate that more focus has to be placed on the managing of e-waste in industry, providing policy directives in relation to how organisations need to prescribe and conform to effective disposal practices of electronic devices that have reached their EOL. Further to this, government, in consultation with various industry role players, needs to look at ways to formalise and regulate the e-waste sector and institute measures to ensure conformance for every part of the value chain.

KEYWORDS

Cybersecurity; Electronic Waste (e-waste); E-waste Policies; Financial Service; Hazardous waste; Waste Electric and Electronic Equipment (WEEE).

DECLARATION

I, Dimitri D. Khumalo, declare that this research report 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 Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Dimitri D. Khumalo Signature: 

Signed at Liefde En Vrede, Johannesburg

On the 27th day of February 2022

DEDICATION

I would like to dedicate this work to my wife and children, it is through your sacrifices and continued encouragement that I was able to finish this study.

Thank you

ACKNOWLEDGEMENTS

Firstly, I would like to thank my Lord and creator, through whom all of this was made possible.

To my wife and children, who greatly supported, encouraged, and believed in me throughout the journey, it's been a tough two years, thank you for your patience and understanding and for always accommodating me when I need to work. Without your unwavering support, I would not have been able to complete this journey.

To all my family and friends; thank you for your words of encouragement and understanding over the last two years, it has been a tough journey, but I appreciate all your support.

To my supervisor, Dr Kiru Pillay, I would like to thank you for your patience, support, guidance, and all the valuable insights you provided throughout this process.

To my syndicate group, fellow classmates, and faculty members, thank you for all your assistance and for creating a conducive environment for learning and knowledge sharing; it was a truly great experience that will always be cherished.

To my employer and all the managers who provided me with the opportunity to study, and to my colleagues, for all your support and encouragement.

Lastly, I would like to thank all the respondents for making themselves available and agreeing to provide valuable insights and contributions to the study.

TABLE OF CONTENTS

ABSTRACT ii

DECLARATION iv

DEDICATION v

ACKNOWLEDGMENTS vi

LIST OF FIGURES x

LIST OF ACRONYMS xi

1 INTRODUCTION 13

1.1 PURPOSE OF THE STUDY 13

1.2 BACKGROUND OF THE STUDY 14

1.1.1 PRIVATE SECTOR CONTEXT 16

1.1.2 PUBLIC SECTOR CONTEXT 17

1.3 RESEARCH PROBLEM 18

1.4 RESEARCH QUESTION 20

1.5 SIGNIFICANCE OF THE STUDY 21

1.6 DELIMITATIONS OF THE STUDY 22

1.7 DEFINITION OF TERMS 24

1.8 ASSUMPTIONS 25

2 LITERATURE REVIEW 26

2.1 INTRODUCTION 26

2.2 BACKGROUND DISCUSSION 27

2.2.1 THE RISING IMPORTANCE AND VULNERABILITIES OF DATA 28

2.2.2 DATA MANAGEMENT AND DATA SECURITY THREATS 30

2.2.3 E-WASTE MANAGEMENT POLICIES 32

2.2.4 E-WASTE AND DATA MANAGEMENT, A SOUTH AFRICAN CONTEXT 34

2.3 PERSONAL AND SENSITIVE DATA AND ICT DEVICE DISPOSAL MANAGEMENT 37

2.4 TECHNOLOGY ADOPTION MODEL 39

2.5 A PRACTICAL APPROACH TO THE APPLICATION OF THE MODELS 43

2.6 RESEARCH PROPOSITIONS 44

2.6.1 PROPOSITION 1 44

2.6.2 PROPOSITION 2 44

2.7 CONCLUSION OF LITERATURE REVIEW 44

3 RESEARCH METHODOLOGY 46

3.1 RESEARCH APPROACH 46
3.2 RESEARCH DESIGN 47
3.3 DATA COLLECTION METHODS 48
3.4 POPULATION AND SAMPLE 49
3.4.1 POPULATION 49
3.4.2 SAMPLE AND SAMPLING METHOD 49
3.5 RESEARCH INSTRUMENT 51
3.6 PROCEDURE FOR DATA COLLECTION 52
3.7 DATA ANALYSIS AND INTERPRETATION 53
3.8 LIMITATIONS OF THE STUDY 54
3.9 TRANSFERABILITY AND DEPENDABILITY 55
3.9.1 TRANSFERABILITY 55
3.9.2 CREDIBILITY 55
3.9.3 DEPENDABILITY 56
3.10 ETHICAL CONSIDERATIONS 56

4 PRESENTATION OF RESULTS 58

4.1 INTRODUCTION 58
4.2 RESULTS PERTAINING TO VULNERABILITIES, DATA MANAGEMENT AND DATA CLASSIFICATION 59
4.2.1 ORGANISATIONAL DISPOSAL PRACTICES TO FACILITATE RESPONSIBLE E-WASTE MANAGEMENT 60
4.2.2 THE IMPACT OF CYBERCRIMES ON AN ORGANISATION WHEN PROPER OF DISPOSAL METHODS ARE NOT ADOPTED 66
4.3 RESULTS PERTAINING TO DRIVING ORGANISATIONAL COMPLIANCE THROUGH POLICY ENFORCEMENT 67
4.3.1 THE IMPACT NATIONAL GOVERNANCE POLICY ENFORCEMENT HAS ON ORGANISATIONAL CONFORMANCE PRACTICES 68
4.4 SUMMARY OF THE RESULTS/FINDINGS 75

5 DISCUSSION OF THE RESULTS OR FINDINGS 78

5.1 INTRODUCTION 78
5.2 VULNERABILITIES AND DATA MANAGEMENT POLICIES 78
5.2.1 DEVICE DISPOSAL PRACTICES AND DATA MANAGEMENT 79
5.2.2 DEVICE DISPOSAL AND CYBER ATTACKS 80
5.2.3 BYOD AND SHADOW IT POLICY MANAGEMENT 83
5.2.4 DATA VULNERABILITIES IN EXTENDED SUPPLY CHAINS 85
5.3 DRIVING ORGANISATIONAL COMPLIANCE THROUGH REGULATORY POLICY ENFORCEMENT 87
5.3.1 FORMULATING REGULATORY POLICY FRAMEWORKS AND MANAGING COMPLIANCE 88
5.3.2 SETTING ORGANISATIONAL POLICY DIRECTIVES AND MANAGING CONFORMANCE 93
5.4 CONCLUSION 97

6 CONCLUSIONS & RECOMMENDATIONS 100

6.1 INTRODUCTION 100

6.2 UNDERSTANDING THE DISPOSAL PRACTICES ORGANISATIONS PUT IN PLACE TO FACILITATE RESPONSIBLE E-WASTE MANAGEMENT 101

6.3 THE IMPACT OF CYBERCRIMES ON AN ORGANISATION WHEN PROPER OF DISPOSAL METHODS ARE NOT ADOPTED 103

6.4 THE IMPACT NATIONAL GOVERNANCE POLICY ENFORCEMENT HAS ON THE LEVEL OF CONFORMANCE OF ORGANISATIONS 104

6.5 RECOMMENDATIONS 106

6.6 SUGGESTIONS FOR FURTHER RESEARCH 107

REFERENCES 109

APPENDIX A: Information sheet 120

APPENDIX B: Agreement form 122

APPENDIX C: Interview guide 123

APPENDIX D1: Research code and transcript association 126

APPENDIX D2: Research analysis data association 127

APPENDIX E: Ethical Clearance Certificate 128

LIST OF FIGURES

Figure 1: A cyber-defence framework (Donaldson et al., 2015, p. 28) 38

Figure 2: UTAUT2 Model (Alqahtani & Braun, 2021) 40

Figure 3: Research process association between proposition, sub-aim, instrument questions and emerging themes (part 1) 60

Figure 4: Research process association between proposition, sub-aim, instrument questions and emerging themes (part 2) 68

Figure 5: UTAUT2 Model (Alqahtani & Braun, 2021) – Social Influence and Facilitating Conditions Constructs applied to analysis 82

Figure 6: UTAUT2 Model (Alqahtani & Braun, 2021) – Habit Construct applied to analysis 85

Figure 7: UTAUT2 Model (Alqahtani & Braun, 2021) – Behavioural Intention construct applied to analysis 97

LIST OF ACRONYMS

BYOD	Bring Your Own Devices
CDO	Chief Data Officer
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agencies
CSO	Chief Security Officer
DDP	Device Disposal Practice
EEE	Electric and Electronic Equipment
EOL	End of Life
EPR	Extended Producer Responsibility
E-waste	Electronic Waste
GITO	Government Information Technology Officers' Council
ICT	Information and Communication Technology
ISO	International Organisation for Standardisation
IT	Information Technology
ITAD	Information Technology Asset Disposition
ITAM	Information Technology Asset Management
MISS	Minimum Information Security Standards
MS	Microsoft
NEMWA	National Environmental Management Waste Act

PII	Personal Identifiable Information
POPIA	Protection of Personal Information Act
SAWIC	South African Waste Information Centre
SITA	State Information technology Agency
SOE	State Owned Enterprises
UTAUT	Unified Theory of Acceptance and Use of Technology
WEEE	Waste Electric and Electronic Equipment

1 INTRODUCTION

1.1 Purpose of the study

This study assesses the vulnerabilities to which organisations are exposed, specifically financial and government institutions, by interrogating the management policies, processes, and procedures for stored data when disposing of e-waste at the end of asset life cycle.

The study further explores how public and private institutions comply to the national legislations, regulations, and standards relating the management and processing of personal and sensitive data, including amongst others, the Protection of Personal Information Act (POPIA) which focuses on the effective management of personal information; the National Environmental Management Waste Act (Act 59 of 2008) (NEMWA) which is focused, amongst other things, on decreasing the amount of waste generated, through the promotion of reducing, re-using, recycling and of recovering waste, and the use of treatment and disposal mechanisms; the Extended Producer Responsibility (EPR) regulation of the NEMWA which seeks to provide assurance that producers of paper and packaging, e-waste and lighting take responsibility for the life span of the products they put out into the market for consumption, from cradle to grave up to the point of post-consumer disposal; the Cybercrimes Act 2020 (Act 19 of 2020) that focuses on cyber related offences created as a result of how data and information, messages, computer devices, and networks are utilised and managed; the Minimum Information Security Standards (MISS) which details the minimum information security measures institution need to have in place when

dealing with sensitive or classified information; and frameworks and standards like the ISO 27000 series of standards for developing best practice organisational improvement guidelines, when developing their Information Technology Asset Management (ITAM) and Information Technology Asset Disposition (ITAD) implementation plans (ERI-Direct, 2018).

1.2 Background of the study

The global landscape has become increasingly dependent on electronic devices and the progressive consumption of technology (Sovacool, 2019). However, this significant growth in technology consumption, driven by rapid innovation, has resulted in a phenomenal decrease in the life span of electronic devices and has created a knock-on effect in the form of electronic waste, referred to as e-waste (Alghazo et al., 2018). This has presented significant challenges for developed and developing countries in how they manage e-waste generated, and in the development of policies to govern the recycling processes (Alghazo et al., 2018).

There have been various descriptions and definitions related to electrical and electronic waste and Sovacool (2019) refers to it as the various components, in different forms of electrical equipment, that have depreciated in value to a point where the economic value of the equipment has decreased to a point lower than that of initial purchase. Tanskanen (2013) adds an additional dimension that takes into consideration aspects of when a device reaches a point of obsolescence, and the owner decides to regard it as waste.

E-waste has far-reaching implications; on the one hand, there is the environmental perspective, and the impacts associated with the toxic

contaminants generated (Mihai, 2021), coupled with the rise in energy consumption of data centres contributing to the total global carbon emissions (Trueman, 2019), and on the other, the security threat perspective and the resultant effects these can have on industries and societies at large.

Studies performed by Forti et al. (2020), show that the worldwide e-waste generated in 2019 is estimated at 53.6 metric tonnes (MT) at a rate of 7.3 kilograms (KG) per capita, which is a growth of 9.2MT since 2014, and is predicted to grow to 74.7MT by 2030. de Froberville (2019) estimated that in 2018, South Africa generated about 6.2KG of e-waste per capita annually and only 12% of this waste was correctly recycled.

Furthermore, studies have shown that the financial ramifications of growth in the e-waste industry has gone up to $7 billion, with the cybercrime industry having an adverse effect and financially draining more than $450 billion annually from a monetary perspective at a global level (Debnath et al., 2019). These two industries are interlaced when proper methods of disposal are not adopted, either by the consumers or by the recycling organisations (Debnath et al., 2019).

To try and manage this rapidly growing industry, countries in the developed economy have been leading the charge in terms of developing policy guidelines and regulations for developing e-waste management systems; those that stand out are notably countries like Switzerland, and the Netherlands, who have been at the forefront in paving the way in this area (Finlay & Liechti, 2008).

Coupled with this growth, and the growth in digital innovation, data has become an increasingly valuable commodity for economies and within society, through a multitude of technological enablers. These very data enablers also have some

form of duality in that, if used correctly, have the potential to create new possibilities for the well-being of organisations and driving strategic organisational benefits, and for communities creating ecosystems of continued evolutionary improvements, but the flip side is that, if poorly managed, data and the analytics around it can create inequality and further expand the digital divide in the digital ecosystem WorldEconomicForum (2020), not losing sight of the environmental ramifications of the increasing number of organisations seeking to become key participants in the present data-driven economy, as a result of emissions generated by these data centres, one of the most substantial pieces of business infrastructure and a key component of this ecosystem (Trueman, 2019).

1.1.1 *Private sector context*

Organisations in the private sector, with specific focus on the financial services industry, handle various customer credit card details, bank accounts, and other forms of sensitive information, they are subject to an even higher degree of regulation than organisations in other industries (ERI-Direct, 2018). The financial industry has an even bigger responsibility to put in place stringent policies, processes, and procedures to ensure the protection of personal and sensitive data at all times, and the effective standards that govern and manage the storage and destruction of data at the various stages of the life cycle of the electronic devices (ERI-Direct, 2018). They have an obligation to ensure key consideration is given to improving and managing their cybersecurity from cradle to grave to reduce the rate of exposure and the level of vulnerability to the threat of cyberattacks (Ameen et al., 2021).

1.1.2 *Public sector context*

In her 2015 national consultative conference, Mrs. Edna Molewa, in her role as Minister of Water and Environmental Affairs of South Africa, highlighted that they had seen a significant rise in the collective amount of e-waste generated by the various government institutions at the various tiers of national, provincial, municipal and state-owned enterprises (Environment, 2015).

In their study, Bob et al. (2017) highlighted that, due to the silo administrative approach followed within the various government institutions, e-waste is being driven through waste management and Information and Communication Technologies (ICT) portfolios, and that no formal centralised structure exists to provide the necessary guidance to the respective departments and municipalities on how to appropriately manage the disposal of electronic equipment, specifically at the End of Life (EOL).

With the varying amounts of sensitive data handled by these institutions, it is paramount that the correct level of policies and procedures, governed by regulations, are put in place to ensure that all ICT devices are properly disposed of and that all data that may have been stored on these devices are destroyed, using the prescribed methods. This is to ensure that all elements of national security are preserved and that state information is not exposed for malicious intent.

.

1.3 Research problem

Countries are increasingly realising the importance of the effective management of e-waste. However, many are yet to develop and formalise practical solutions and recognise the importance of classifying and seeing it as a hazardous waste stream across the various industry sectors (Finlay & Liechti, 2008).

In the current South African landscape, there is no specific legislation that explicitly focuses on e-waste (Finlay, 2007). Waste in South Africa, of which e-waste is a component, is currently governed by approximately 13 pieces of legislation, and it is the introduction of Section 18 Regulations to the National Environmental Management Waste Act, published on 5 November 2020, focused on electric and electronic equipment (EEE), that specific reference to the EPR scheme for the electrical and electronic equipment scheme is provided for in the act (SAWIC, n.d).

This is coupled with policy guidelines and legislation related to e-waste management systems and to creating a society that is driven by sustainable recycling habits, as mentioned by (Finlay & Liechti, 2008), and (Tanskanen, 2013). Another area of key consideration is the requirements centred around the mechanisms that need to be put in place, on how to manage cybersecurity threats for the e-waste generated and disposed of in these processes, given the large volumes of sensitive data (including contacts, e-mails, banking details, customer information, photographs, and videos, etc.) that are stored and processed on ICT equipment (Ameen et al., 2021).

Forgor et al. (2019) note that through the application of simple data recovery software, it was found that it was easy to retrieve remnant data from a large number of disposed of electronic devices even after the application of basic formatting procedures, which creates the inherent risk of individual and organisational information being open to being recovered and exploited by individuals who have malicious and criminal intentions.

This is further supported by Mihai (2021), who noted that during the E-waste World Conference, John Shegerian, the CEO of an electronics recycling company denoted e-waste hacking or the extraction of information from e-waste devices as “an overlooked crime” and “the greatest little secret of the cybersecurity world” (Mihai, 2021, para. 3), with this problem contributing to the growth in the global annual cost of cybercrimes.

With the increase in innovative IT applications and services being developed and introduced, cloud-based services are also becoming a growing phenomenon due to the ease of accessibility (Haag & Eckhardt, 2017). Employees are now looking to this growing trend of Shadow IT, and various other solutions-based applications and utilising these within the organisational frameworks, which are not formally approved, and have the potential of exposing the organisation to a number of security related risks (Silic et al., 2016).

The doors have been further widened as organisations have looked to various cost saving initiatives, while creating a collaborative ecosystem by allowing employees to use their own personal devices (Huffington-Post, 2017). The current pandemic has further accelerated the work from home situation that most

organisations have been grappling with for the past few years as they have tried to manage the cost of office space and the work-life balance of employees.

This phenomenon of “Bring Your Own Device” (BYOD), as described by Eslahi et al. (2014), enables employees, through the use of their personal devices to connect to the enterprise network and, and enable them to fulfil their daily work-related activities, irrespective of place or time. This, however, as pointed out by Morrow (2012), creates a great challenge for these organisations as it allows corporate data to be accessed or retrieved from devices that are not managed and controlled by the IT department. Furthermore, global organisations have had to contend with retrofitting their BYOD policies in accordance to various local laws or policy frameworks set out in the various countries in which they operate, ensuring these organisations minimise the potential for data leakage, data theft and not effectively complying to regulatory compliance (Veljkovic & Budree, 2019).

This is mainly because employees do not at all times possess the same level of security to safeguard their devices and the information stored on them (Huffington-Post, 2017).

1.4 Research question

As per the problem defined, the main purpose for this study is to assess how data (both personal and sensitive) is managed within private sector organisations and public sector institutions when disposing of electronic ICT equipment, when these devices have reached their EOL.

I. Sub-aim 1: What disposal practices do public and private sector organisations have in place to facilitate responsible e-waste management for the different categories ICT devices?

II. Sub-aim 2: What impact do cybersecurity vulnerabilities have on organisations when proper methods of disposal are not adopted either by the public and private sector organisations or by the third-party recycling institutions?

III. Sub-aim 3: What impact does the enforcement of national governance policies have on the level of conformance of public and private sector organisations to policies governing the cleansing of data on electronic devices before disposing of them when they have reached their EOL?

1.5 Significance of the study

The study identifies the gaps in the policies in relation to the vulnerabilities in the disposal of e-waste within the South African financial service sector, government institutions and e-waste disposal companies, specifically focusing on the compliance to cybersecurity regulations, like the cybercrimes act and POPIA detailing the management of data breaches in the destruction of data contained or stored on electronic devices.

The key focus here is to detail how through the development of clear regulatory policies and frameworks, organisations are able to develop effective ITAM and ITAD implementation plans (ERI-Direct, 2018), which are aligned to the waste disposal and data destruction policies and procedures of their third-party e-waste recycling suppliers or vendors. Coupled to this, to assess the active involvement

of government agencies to ensure that all parties throughout the value channel comply to, and are held accountable to ensure that all disposal activities are done within the confines of the regulatory frameworks.

This paper explores the nature of e-waste in the private and public sectors, and investigates regulatory vulnerabilities centred on e-waste, when disposing of electronic equipment. The study further explores the governance related dimensions of:

Dimension 1: Assessing the asset management with specific focus on the management of data, and the disposal behaviours for the various electronic devices utilised by employees when they have reached their EOL as classified by the various organisational policies.

Dimension 2: Interrogating the various acts and regulations to assess the degree of responsibility placed on institutions for the management of personal and sensitive data, and to what extent they are held liable for any mismanagement.

1.6 Delimitations of the study

This research study is aimed at the South African financial services industry, and various government institutions, addressing the cybersecurity related vulnerabilities created when assets are not effectively disposed of in line with defined regulatory policies when they have reached the end of their life.

The study addresses the following areas by focusing its investigation on:

I. The interrogation of the various organisational policies and procedures relating to the management of data and the key organisational

responsibilities to ensure that this data is effectively disposed of when discarding ICT equipment.

II. The effective management of ICT equipment within the public and private sectors that have been classified as e-waste and reached the end of their useful life.

III. The application and compliance to regulatory policy guidelines, frameworks, and international standards for the management of e-waste and the effective disposal of the equipment and the data that may still be stored on the devices.

Additionally, the study focused on the executive layer of organisations including Chief Information Officers (CIOs), Chief Digital Officer (CDOs) and Directors, Deputy Directors, and senior management teams within the various public and private sector institutions responsible for the formulations and governance of ITAM and ITAD implementation plans (ERI-Direct, 2018), and their third-party e-waste recycling suppliers or vendors contracted for the management and disposal of e-waste, and the destruction of data stored on those assets.

1.7 Definition of terms

Term	Definition
Bring Your Own Devices (BYOD)	A phenomenon employed by organisations that enable employees, through the use of their personal devices to connect to the enterprise network and, and allows them to fulfil their daily work-related activities, irrespective of place or time (Eslahi et al., 2014).
Cybersecurity	Defined as technological measures or practices that have been put in place to aid in the protection of data, computer programs, computer data storage mediums or computer systems to eliminate/elevate the damage or interference that emanates from cyber related crimes (Alghazo et al., 2018).
E-waste	The various components, in different forms of electrical equipment, that have depreciated in value to a point where the economic value of the equipment has decreased to a point lower than that of the initial purchase (Sovacool, 2019).
Extended Producer Responsibility	Defined as the responsibility that an individual/organisation bears the for that they any product produced which is extended to the stage or point after it has reached the product's end of life cycle or usefulness as defined by the consumer (SAWIC, n.d).
Information Technology Asset Disposition (ITAD)	Outlines the defined plans instituted by organisations on how they manage the disposal of their IT assets (ERI-Direct, 2018).
Information Technology Asset Management (ITAM)	Outlines the defined business practices put in place to manage and support organisational assets infrastructure throughout their lifecycle and optimise strategic decision-making within the organisations IT environment (ERI-Direct, 2018).

1.8 Assumptions

1. The executives, Chief Information or Chief Data Officer (CIO/CDO), and the Directors, Deputy Directors, and senior management teams within the various public and private sector institutions are open and free to discuss their ITAM and ITAD implementation plans and identified vulnerabilities in relation to defined policy frameworks and their level of compliance
2. Individuals from the various e-waste recycling companies are willing to participate in the study and accurately and truthfully answer questions related to:
    I. Their process related to the compliant disposal practices of customers' assets and the data stored on those assets
    II. The effective management and disposal of e-waste material

2 LITERATURE REVIEW

2.1 Introduction

There have been numerous studies that have sought to investigate the various facets of e-waste. The majority of the research conducted has sought to explore and investigate the hazardous impact of e-waste on the environment and on society at large. Some of the studies have sought to look at the aspects relating to government involvement and the specific policies they have put in place to manage the entire e-waste value chain.

A number of authors such as Alghazo et al. (2018), Ameen et al. (2021), EACO (2013), Finlay (2007), (Friedmana & Hoffman, 2008), and (Kumar et al., 2017) have recognised through their research that due the limitation in their policies and procedural guidelines, organisations have been left exposed to varying levels of cybersecurity vulnerabilities, specifically financial and government institutions, and gaps in the destruction and management of stored data when disposing of e-waste at the end of asset life cycle could be a significant threat to these institutions.

The approach that is followed in this literature review is to assess and synthesise scholarly literature of peer reviewed journals to seek to understand whether the correct measures have been put in place to assist in the governance of private and public institutions in ensuring the effective management, and responsible destruction of data when disposing of e-waste devices after they have reached their EOL.

The key focus is centred on the South African public and private institutional policies that govern the destruction of data contained on electronic devices used in the private and public government sectors, and the impact of cybersecurity threats that may result from the ineffective management e-waste processes (with attention being placed on compliance requirement, people, process and technology (Donaldson et al., 2015)) within these institutions. This is further extended to all third-party service providers involved in the value chain, whose operational activities are required to ensure all inherent risks are mitigated and a good reputation is maintained for all parties involved (Jones, 2009).

2.2 Background discussion

The intense competition between organisations within the electronics industry has led to a steep rise in the time to market and release of new and upgraded electronic products (Plambeck & Wang, 2009). This has yielded significant benefits with regard to technology advances and the development of constantly evolving digital solutions and platforms.

However, these advances have come at a significant price, as the global e-waste numbers over the last decade have steadily been growing at an unprecedented pace. In his article, Upton (2021) highlighted that the electronics industry in 2020 was a key contributor to the generation of at least 53.6 Mt of e-waste globally, which was a sharp rise of 21% over the previous five years (Upton, 2021).

The plight regarding the growing concerns around e-waste was further exacerbated ahead of the 2021 G-7 summit when a sculptor emulated Mount Rushmore, when he depicted the leaders of the G-7 using e-waste material

(BritishBroadcastingCorporation, 2021). The sculptor's intentions was to send a message that illustrates the radical need for electronic devices to be made in a way that allows them to be easily reusable or recyclable with a drastic reduction on disposal (BritishBroadcastingCorporation, 2021).

Added to the growing concerns centred around e-waste, is an area that focuses on the management of cybersecurity. With a specific focus on the cyber-related threats and the various mechanisms that have been put in place, to govern how data is managed and cleansed or removed from electronic devices when disposing of e-waste, given the large volumes of sensitive data (including contacts, e-mails, banking details, customer information, photographs, and videos, etc.) that are stored and processed on ICT equipment (Ameen et al., 2021).

According to figures from the 2021 G-7 summit, as published by CXOtodayNewsDesk (2021), cybercrimes committed globally in 2020 reached a staggering 69% which was up from the previous year's total, which saw an increase in the level of complexity-related cyber-attacks, cybercrimes and other risks as the associated cyber-attackers had considerably improved their game, meaning that considerable interventions by government and organisations need to be put in place to curb this seemingly uncontrollable upsurge.

2.2.1 The rising importance and vulnerabilities of data

With the growth in digital innovation, data has become an increasingly valuable commodity for economies and within society through a multitude of technological enablers. However, like all things of value, the demand for data has risen both for

the betterment of our livelihoods, but also for those who seek it for ill-gains and malicious intention, due in part to it being unregulated, with no clear agreements around issues like access and ownership (MacFeely et al., 2020). This has created opportunities for cyber criminals to continually seek for new avenues and process and system vulnerabilities that could be exploited to work in their favour.

Given the growing importance of data and its evolving prominence, data has been elevated to a level where it is even seen as a new form of a commodity that can be traded. However, there is a need to ensure that with this growing demand and value placed on data, we find mechanisms to ensure that the well-being of people are protected and that data is analysed and used to gain insights that will facilitate an improved way of life, but at the same time, ensure that their privacy is protected and data appropriately managed, from cradle to grave, to minimise any misuse and abuse and ensure that data is safeguarded against all vulnerabilities and threats (WorldEconomicForum, 2020).

The scale and impact can be illustrated in cases like the Equifax data breach where cyber attackers, due to a flaw in one of their applications, were able to access the personal identifiable information (PII) of over 143 million customers belonging to Equifax, between May 2017 and (Wattles & Larson, 2017). A further example was in the case of Liberty Life, one of South Africa's biggest data breaches; where through a breach in its email repository, the personal details of over 30 million clients were accessed and a ransom requested, at the threat of leaking the data online (IOL, 2019); this and subsequent breaches within the South African landscape made organisations sit up and start re-looking the

importance of effective cybersecurity policies and plans to safeguard themselves against these growing threats.

2.2.2 Data management and data security threats

The privacy of one's data has been a hotly debated topic, with the recently updated POPIA act striving to ensure that one's personal information is properly managed and processed by public and private institutions (DLAPiper, 2021). An element that has also been brought to the fore is how these institutions and the third-party suppliers handling and managing their devices and PII comply with the various conditions defined in the act (Adams et al., 2021).

This has become more prevalent with the usage, storage, and accessibility of data on electronic devices used for day-to-day interaction and transactions, however little emphasis is placed on what happens to data once a device no longer has a meaningful purpose for the owner and is deemed to be obsolete or has reached its EOL (Schafer, 2014).

Schafer (2014) further notes that the worrying factor currently being faced by developed and developing countries is the rate at which e-waste is generated and the technical mechanisms available to securely dispose of discarded devices that are significantly outpaced by technological and digital innovation of the devices being manufactured and brought into the market.

This ties into the notions discussed by Ichikowitz and Hattingh (2020), who highlight the various interdependent components of DDP, with specific focus placed on the flow of devices and where these devices ultimately land up once disposed of. Added to this is the level of assurance placed on mechanisms to

facilitate the prevention of any reconstruction and unauthorised access of these electronic assets or devices during disposal (Schepers & Novazi, 2020).

The rise in digital devices has further been fuelled by the changing dynamics of the workforce who have gradually migrated to the use of mobile devices, to allow for a greater flexibility in the execution of tasks in this digitally connected world in which we are living (Friedmana & Hoffman, 2008), coupled to this is the growing trend of BYOD which has enabled employees the ability to connect their personal ICT devices to their enterprise networks and enabled them to fulfil their daily work at any physical location, in accordance to their desired schedules (Eslahi et al., 2014).

However, with this level of flexibility, Friedmana and Hoffman (2008) also point out the inherent risk involved in these advancements and the security vulnerabilities associated with the loss and unintended access to customers personal identifiable information. This can also be linked to individuals and their belief that the security features on their devices possess enough security to protect their data and that their devices are secure and invulnerable to any threats (Alqahtani & Braun, 2021; Escobar-Rodríguez & Carvajal-Trujillo, 2014).

Debnath et al. (2019) and Thing and Tan (2012), in their papers all look at the specific mechanisms of retrieving data from devices, with specific emphasis placed on reverse engineering techniques that could be employed by criminals to exploit and use to their benefit, security vulnerabilities of these electronic devices, specifically those that have been discarded as e-waste.

It has become imperative that organisations, both in the public and private sectors (including the individuals employed in these institutions) and the third-party

service providers contracted to dispose of e-waste, become more aware regarding the data privacy with more attention placed on EOL devices to ensure the correct levels of protection are put in place to secure data throughout the various phases of the value chain, including mechanisms to deal with the unregulated market and devices ending up in landfills (Alghazo et al., 2018). Specifically, given that criminals are increasingly looking to exploit the growing avenue of e-waste dump sites where they are likely to obtain or purchase devices that potentially contain highly sensitive data and use this in an elaborate scheme to request ransom or use it for fraud and identity theft related crimes (Whitty, 2018).

This could also have an adverse impact on the credibility of the organisation in relation to their corporate reputation and brand image if found that they could have played a more instrumental role in ensuring that all mitigation strategies and procedural plans have been catered for and put in place to eliminate any potential threats and vulnerabilities of data leakages at EOL of devices (Heeks et al., 2014).

2.2.3 E-waste management policies

The 21st century has seen a rapid rise in the advance of technology, which has sparked the development of electronic devices to support these technological advancements and bring about an improved way of life (EACO, 2013). With this radical growth, organisations have had to keep abreast with the demands of these evolving technologies, but also strive to satisfy the rising needs of the consumer for better and enhanced features and accessories (Perkins et al., 2014). This has

led to the life span of devices drastically decreasing, resulting in the rise of e-waste being generated (Perkins et al., 2014).

This rise in e-waste is due to the changing economic and socio-economic climate, fostering technology inclusivity and trying to bridge inequalities and also drive policy certainty driven by a constantly evolving political landscape, (Heeks et al., 2014); this has meant that governments ensure that the correct policies are adopted and put in place to drive the effective management of e-waste. Government's main function is to develop legislation that defines effective ways of managing e-waste, and to drive the enforcement of regulations through all the parts of the value chain (Ikhlayel, 2018).

Sabillon et al. (2016) detail that this could be driven through the establishment of governmental platforms that allow their institutions to communicate specific elements of defined regulations. These are key determinants for successful policy implementation in organisations (Sari et al., 2021), which ultimately drive towards the right level of compliance through effective management, enabling effective policy enforcement (Ghosh et al., 2016).

This could further be extended to the government becoming more focused and deliberate with regard to specific e-waste policy development, appreciating the fact that there are various complexities related to e-waste and data management streams (Maphosa et al., 2020).

Allam et al. (2014), Borthakur and Govind (2017), Downer and Bhattacharya (2015), Gu et al. (2017), Patil and Ramakrishna (2020), and Veljkovic and Budree (2019) point to the fact that there is great reliance on user awareness

and education for compiled and implemented policies to be successfully rolled out and not as a once-off initiative, for employees to play a more essential role in the management of cybersecurity, e-waste, and DDP.

Ultimately, this should be driven through regular audits and/or compliance assessments, as this may change the attitudes of institutions if faced with the threat of potential fines, loss of operating licences, and imposed sanctions, as a result of non-compliance with various prescribed regulations (Heeks et al., 2014). Sovacool (2019) highlights that those policies are developed and put in place at a national level and need to be put into action, not just exist as documented policies on paper only, but rather more should be done by government and institutions to enforce adoption and compliance of the specific policies to ensure the better management of e-waste.

2.2.4 E-waste and data management, a South African Context

E-waste management is a phenomenon that is generating a lot of attention in both developed and developing nations. South Africa too, has started sitting up and paying more attention to the growing challenges presented by e-waste. Much research has been conducted, focusing on the diverse array of elements like the environmental issues crated, the lack of adequate policies to drive effective e-waste disposal and the protection of information at EOL, and e-waste management strategies to guide organisations in relation to e-waste management (Lawhon, 2013).

In his paper, Borthakur (2020) indicates that in recent years, little has been done in terms of research around e-waste specifically in the South African context,

which he substantiates by providing an annual view of the e-waste distribution research conducted in South Africa between 2006 to 2018.

, in his research, raised concerns that no specific legislation that focused specifically on e-waste, had been put in place in the South African landscape. This is seen where the waste in South Africa is currently governed by 13 pieces of legislation which can be accessed from the SAWIC, none of which have a specific focus on e-waste, as it is seen in the ambient of general waste as also detailed by (Bob et al., 2017).

Besides the concerns around how South African regulations governing the disposal of e-waste has an influence on organisational policies in the financial services and government departments, another area that requires focus is the management of data, specifically at the juncture where electronic devices have been discarded, and as detailed by Warner et al. (2012, p. 13), understanding the impact the end-user consumer has on their various approach and decisions on where and how they dispose of their IT and electronic devices.

I. Management in the private sector contextualised

With the continually changing technology landscape, organisations and their employees are doing everything possible to remain abreast and adapt to these changes. This is evident in cloud-based services that drive ease of accessibility for the end-user (Haag & Eckhardt, 2017), like Shadow IT hardware or other solutions based activities utilised by employees. Silic et al. (2016) and Eslahi et al. (2014) denote the rampant rise in the use of BYOD, facilitating the use and management of electronic devices by their employees.

This is compounded by how global organisations contend with and retrofit their BYOD policies in accordance to various local laws or policy frameworks set out in the various countries in which they operate (Veljkovic & Budree, 2019), but also how they try to minimise the challenges and various risks of data exposure and the vulnerabilities that could adversely affect an organisation's security systems and infrastructure, their employees could be exposed due to remote working (Chigada & Daniels, 2021; Washtell, 2022).

However, besides the e-waste governance aspects that need to be set up to manage these trends, a constant concern that remains a challenge for organisations, specifically those in the financial services industry, for devices that are at their EOL and at that part of the value chain where they have to be disposed of, is the focus on the ITAD plan and procedures, that have been put in place to effectively secure and control all sensitive corporate and client information that may still be stored on these devices (Morrow, 2012).

The ITAD plan is critical in providing the organisation with a framework detailing the steps required to manage the disposal of IT assets, and the importance of management, through visible actions, formal directives and continued engagement, to ensure that employees remain compliant and conform to all defined frameworks, (Connolly et al., 2016); (Dols & Silvius, 2010); aligned with various other regulatory policies and statutory frameworks that will cover requirements detailing how private and sensitive data will be safeguarded during the disposal process, including details surrounding the management of, internal registry and reporting structures of assets, internal and external data cleansing and destruction, and third-party providers contracted to assist with the

transportation and disposal of assets (ERI-Direct, 2018). This in turn, will facilitate operational activities that ensure all inherent risks are mitigated and a good reputation is maintained for all parties involved (Jones, 2009).

II. Management in the public sector contextualised

According to the structural make up within the various government departments, it has been found that a clearly defined management structure providing guidance for e-waste including disposal procedures, does not formally exist (Bob et al., 2017). ICT policies that govern the purchase, and use of electronic devices provide guidance to the respective ICT structures in this domain, but not much has been done to manage the equipment when they have been classified as e-waste as they are deemed to no longer possess useful value, which has implications on how this is currently being administered within the various departments (Bob et al., 2017).

Of specific concern is also the process related to data destruction of devices, specifically those environments that deal with sensitive data that could pose a threat to national security.

2.3 Personal and sensitive data and ICT device disposal management

As depicted by the various authors, and as denoted in the literature review, the main purpose for this study is to assess how data (both personal and sensitive) is managed within private sector organisations and public sector institutions when disposing of electronic ICT equipment, when these devices have reached their EOL.

Through the applications of the cybersecurity framework, as detailed in Figure 1 below, defined by Donaldson et al. (2015) is a comprehensive set of technical, business, and people skills, that all work in synergy to put together an efficient organisation-wide cybersecurity mission that can be used to protect and safeguard the organisation against all cyber related vulnerabilities and threats, utilising all resources to achieve the desired objectives.

The researcher seeks to illustrate how the application of this model can be used by institutions to develop and formulate robust ITAD and ITAM implementation frameworks which will facilitate how e-waste and the disposal of data is managed in this end-to-end value chain cycle.



Figure 1: A cyber-defence framework (Donaldson et al., 2015, p. 28)

The framework starts by considering all elements, both internal and external to the organisation, that will serve as input factors into developing comprehensive Compliance Requirements that will serve to provide the necessary strategic guidance, translated into executional ITAM and ITAD plans (Donaldson et al., 2015, p. 27). These are underpinned by the people who make all this possible;

given the correct level of guidance and support; through their day-to-day interactions and engagements (Donaldson et al., 2015, p. 28). All of this is orchestrated through the correct processes and procedures being defined, developed, and put in place with frequent reviews to continually improve as new developments are made (Donaldson et al., 2015, p. 28). This is supported through the implementation and utilisation of technologies to facilitate and drive the implemented plans, and to provide the correct level of monitoring and reposts to allow for the correct level of decisions to be made (Donaldson et al., 2015, p. 28).

2.4 Technology adoption model

The Unified Theory of Acceptance and Use of Technology (UTAUT) is a theoretical model just over a decade old, that has, through extensive work, synthesised previous theoretical models that predict the use and acceptance of technology (Venkatesh et al., 2016). With the inclusion of additional constructs; hedonic motivation, price value and habit, the model was further enhanced to formulate the UTAUT2 Model (Chang, 2012), as detailed in Figure 2 below.

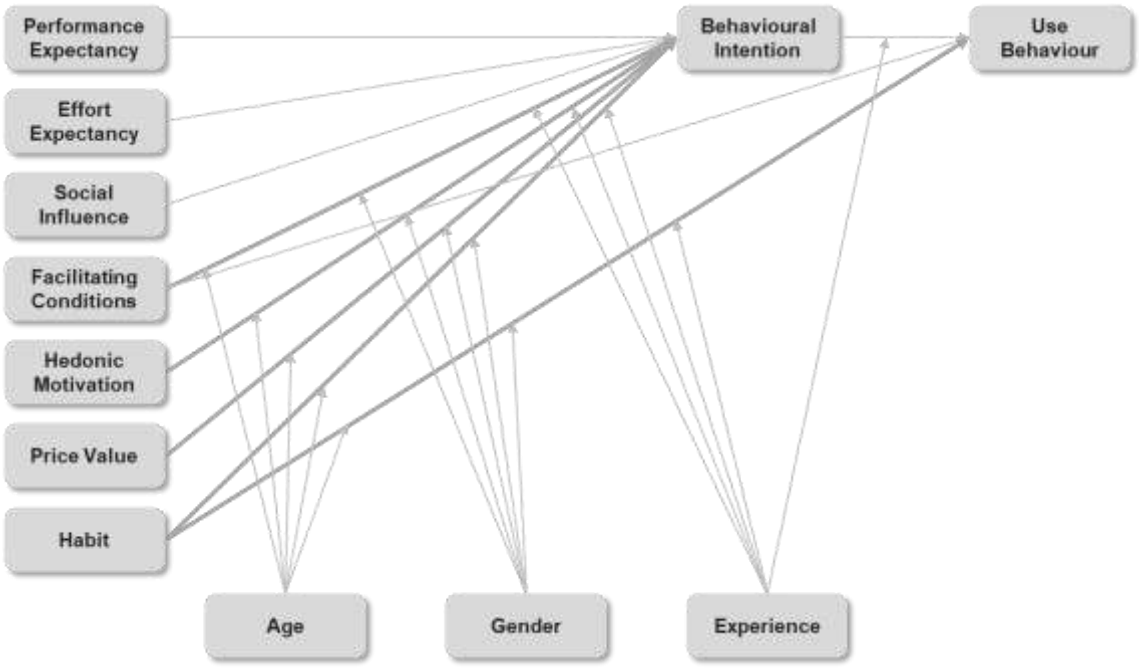


Figure 2: UTAUT2 Model (Alqahtani & Braun, 2021)

The UTAUT, with its adaptation and enhancement, focused at driving attention towards technology use, is found to be more applicable for employee use (Alqahtani & Braun, 2021). Using the UTAUT2, the research explores the factors that affect the adoption of technology which has a significant bearing on the premise set out by Venkatesh et al. (2016), that denotes that an individual must first use a technology before they are able to achieve a desired outcomes, like improved in employee performance.

Through our study we explore how institutions endeavour to develop organisational policies and implement processes and procedures that will be effected by the people, and ensure that these are adequately understood, to allow for the right levels of conformance to the security measures and drive adhere to compliance requirements to achieve a successful level of cybersecurity (Donaldson et al., 2015) in relation to the management of data at equipment EOL, with the focus being placed on the model's seven constructs (Alqahtani & Braun,

2021), and the relationship between the respective moderators used to predict a user's behavioural intention to use a technology and the actual utilisation of the technology, in an organisational context (Venkatesh et al., 2016).

Chang (2012) denotes that, age, gender, and experience are posited as extraneous moderating variables that have a direct influence on the four fundamental constructs; hedonic motivation, price value, and habit and which are moderators to the factors corresponding to the usage behaviour and intention of technology.

I. Performance expectancy

Performance expectancy, as defined by Alqahtani and Braun (2021) and Escobar-Rodríguez and Carvajal-Trujillo (2014), deals with the concept of explaining how technology is anticipated to benefit the users when performing varying activities in different capacities and different ways to achieve an intended result.

II. Effort Expectancy

Effort expectancy is defined as and focuses on the relative ease or amount of effort related to the use of a technological system (Alqahtani & Braun, 2021; Escobar-Rodríguez & Carvajal-Trujillo, 2014).

III. Social Influence

A person's perception is based on social and societal influence, which focuses on how individual's views certain behaviours based the opinions of people within their close network and what they may think if they perform or do not perform a

set behaviour in relation to the use of a technological system (Kan & Fabrigar, 2017).

IV. Facilitating Conditions

Facilitating conditions are defined as an individual's perceived belief that resources in relation to organisational and technical infrastructure and performance behaviours, exist to support the utilisation of a technological system (Alqahtani & Braun, 2021; Escobar-Rodríguez & Carvajal-Trujillo, 2014).

V. Hedonic Motivation

Defined by Kan and Fabrigar (2017), as voluntary actions contextualised by certain factors of action, target, context, and time that will drive the set actions that are performed by an individual in a specific circumstance when using a technological system.

VI. Price Value

Simply defined, it is a user's positive perception in relation to the benefits derived from technology and the primary impact on the user's intention to bear the cost of that specific technology (Chang, 2012). This is essentially seen as a cost-benefit analysis by the user, which subsequently impacts the user's usage intention regarding a technology (Alqahtani & Braun, 2021).

VII. Habit

It can be categorised as the performance of an act, generally an automatic execution, based on an individual's past experience. (Alqahtani & Braun, 2021).

VIII. Behavioural Intention

The likelihood that individual's within the organisation will perform or behave in an intended way (Kan & Fabrigar, 2017), thus focusing on how likely organisations are to comply to regulatory policies based on the perceived behaviours of the individuals within these organisations' likelihood that they will perform a behaviour based on the other variables that are interlinked.

2.5 A practical approach to the application of the models

Theoretically, this study demonstrates an emerging relationship between technology adoption and cybersecurity compliance, which adds to the development of compliance mechanisms for security frameworks of an organisation of public or private or government institutions (Alqahtani & Braun, 2021). The drive is to understand how the constructs of the UTAUT2 interlink to core elements of the cyber-defence framework, the formulation of robust ITAM and ITAD implementation plans, and the impact they have on how people in organisations, based on specific behaviour and built-in deterrence mechanisms, as detailed in the construct of the deterrence theory enables the institutionalisation of cybersecurity policies and encourages employees to adopt these policies through effective process and use of technology, making their behaviour more compliant (Alqahtani & Braun, 2021; Kuo et al., 2020; Marks, 2011).

2.6 Research Propositions

Propositions are statements or phrases that look into the relationships between concepts. A proposition details the logical association between certain concepts by stressing a universal connection between these defined concepts (Zikmund et al., 2009, p. 42).

2.6.1 Proposition 1

Assessing the vulnerabilities in the management of e-watse with specific focus on how data is managed when disposing of electronic devices utilised in public and private institutions, when they have they have reached their EOL, as classified by defined organisational policies.

2.6.2 Proposition 2

Assessing how better enforcement of regulatory policy, impacts and has the potential to improve the compliance and responsible behaviour of organisations in relation to the proper management of data during the disposal of e-waste equipment at the EOL.

2.7 Conclusion of Literature Review

There has been a growing realisation of the importance of effective management of e-waste policies and strategies within global and more specifically, South African institutions, specifically around the management of data and e-waste devices when being disposed of.

Numerous studies have sought to investigate the multiple aspects of e-waste and personal and sensitive data with specific focus on the rising importance of data, the approaches followed in relation to how data is managed, and the management of e-waste devices, throughout their respective life cycle phases with explicit emphasis on the end-of-life phase.

Through the synthesis and assessment of scholarly literature and peer-reviewed journals, the researcher has sought to illustrate the different aspects that have been focused on, in relation to these topics, and how continued advances in the technology landscape have brought about enhancements, both to organisations and society, in terms of the utilisation of technologies and the increased importance of data. However, this has also come with unintended challenges, specifically the threats of malicious access to the data generated and utilised on these devices, due to vulnerabilities created within the ecosystem.

3 RESEARCH METHODOLOGY

3.1 Research approach

The literature review discusses the elements that impact the way in which regulatory policy guides and shapes how organisations and institutions implement ITAD strategies, and the implications that proper enforcement can have on how these are complied with.

This study was broadly qualitative in nature, which utilises an inductive style in the exploration and formulation of a specific understanding into how individuals or groups of people place meaning and significance to social or human problems they are faced with in their daily interactions (Creswell & Creswell, 2018).

This research utilised the interpretivist view, a branch in the qualitative paradigm, which is considered a method of social enquiry and places its focus on the human element to formulate social constructs based on the reality of the subjects (Balushi, 2018). In our paper, the interpretivist technique, specifically focusing on the selection of individuals based on their roles and expertise in their organisations, is used to explore how South African public and private institutions adopt legislation and policies, directives, frameworks and standards when developing their ITAM and ITAD implementation plans to ensure compliance relating to the management of personal and sensitive data at equipment EOL.

3.2 Research design

The study used the phenomenological research design, defined as a study seeking to understand the perceptions, perspectives of the research subjects and to obtain an understanding of how they view a particular phenomenon (Pathak, 2017). The study specifically looks at Hermeneutic Phenomenology which explores the personal experience described through interpretation of the lived experience of human individuals to create meaning and achieve a sense of understanding of their various experiences in the environments they are exposed to (Pathak, 2017).

As defined by Pathak (2017), through this methodology, the study sought to understand how certain perspectives and perceptions influence the adherence and compliance in relation to how data is managed in respect to sensitive and PII when disposing of electronic devices and the impact regulatory policies have on how the organisational frameworks and policies are formulated.

Based on this, the defined propositions would lead to the deduction and interpretations of certain outcomes based on the outcomes of the data collected, surrounding the views of the respondents in the formulation and applications of varying measures and mechanisms to ensure adequate measures are in place to manage and comply with regulatory policies in relation to cyber threat and/or vulnerabilities of personal and sensitive data during the disposal of e-waste devices that have reach their EOL.

3.3 Data collection methods

The data collection method utilised for this study was semi-structured interviews conducted with the various respondents, selected as part of the target population.

It was conducted through one-on-one conversational type engagements or interactions with selected respondents, the semi-structured interviews utilising a combination of closed and open-ended type questions, that were in most instances, followed up with a few probing questions, facilitating an engaging type dialogue to thread through the topic at hand and enabling the interviewer to delve into issues that would not have been uncovered through a more formal and scripted type dialogue (William, 2015). This approach of discussion in the qualitative approach, facilitated the exploration of a defined problem, which ultimately assisted the researcher in gaining an in-depth understanding, through these interactive discussions, of the various experiences, and views in relation to the topic and other contributing factors that could have a bearing on the study (Creswell & Creswell, 2018).

Given the Covid 19 pandemic restrictions at the time, the use of online technology was considered as an alternative option. However, as highlighted by Balushi (2018), this method comes with its own challenges, specifically the limitations in visual and non-verbal cues which would have been more evident in a face-to-face setting that would aid in providing added context to the interview. However, this was managed through careful interpretation of what was said and how it was said when analysing the contents of the interview session (Balushi, 2018).

3.4 Population and sample

3.4.1 Population

The target population that was considered for this study were predominately:

I. Executives (CIO/CSO), deputy CSO, data and security Department Heads, and infrastructure, data and security Senior Managers within institutions in the financial services sector,
II. Director of IT security and Head of Departments for Infrastructure and security management within the government institutions and State-Owned Enterprises (SOE's) e.g. State Information Technology Agency (SITA), Government Information Technology Officers' Council (GITO), State Security Agency, etc. within the public institutions,
III. The CEO's and owners of the e-waste recycling companies situated in the Gauteng province in South Africa.

3.4.2 Sample and sampling method

Purposive sampling, also defined as judgemental or expert sample, is a non-probability sample with its key focus being the ability to produce a sample that can be rationally presumed to be representative of the population (Campbell et al., 2020). In an attempt to validate its use or selection, one assesses its ability to ensure an effective sampling frame for the data collected, utilised, and evaluated to achieve the defined outcomes of the research study, which aids in improving the rigour of the study and adds an element of trust to the results from the data (Campbell et al., 2020). Purposive sampling was used in this study.

According to its varying categories, purposive sampling has six distinctive categories. For the purpose of this study, we focused on the homogeneous sampling as it places its focus on one specific sub-group where their members share a very particular relation or have very distinctive similarities, e.g. occupation or level within an organisation's structure (Dudovskiy, n.d).

There were a limited number of primary data sources who were able to significantly contribute to the study (Dudovskiy, n.d), who in this case, as indicated in the sample population, was limited to particular individuals (based on position) from the financial services sector, government institutions and SOE's, and e-waste recycling companies.

From the target population that was considered for the study, the researcher initially approached 23 individuals to participate in the study, however due to varying reasons, which stemmed from either:

I. the individauls being reluctant, due to potential exposure risks (highlighting that not all their paperwork was 100% in order),
II. the topic being closely related to clauses within non-disclosure agreements they had signed,
III. lengthy approvals within the various organisations, resulting in respondents losing interest or being unable to assist, to
IV. not responding to communication regarding the confirmation of intention to participate in interviews (to a point of avoidance).

This ultimately resulted in the commitment of 12 respondents who participated in the study, having been selected based on the specific roles and experiences they fulfilled within their respective organisations.

From some of the sessions, certain of the individuals indicated that though their roles were in line with the prescribed positions for the sample selections, certain of the functions and responsibilities were not in their executional areas, and based on this, three of the respondents referred the researcher to other individuals within their respective organisations who would be of assistance, based on the specific questions posed during the interview sessions. This approach thus employed snowballing sampling, which is categorised by Bhardwaj (2019) and , as chain sampling, referral sampling, chain-referral sampling or sequential sampling, which is used where one respondent identifies other respondents from their network or acquaintances who might be suitable for participation in a study.

The interview sessions were conducted over a duration of between 45 minutes and 60 minutes and were all recorded (through consent) and transcribed post the interview session and analysed using the ATLAS.ti qualitative data analysis computer software tool.

3.5 Research Instrument

The research instrument utilised for the study was based on semi-structured interviews made up of a combination of closed and open ended questions, and included 15 questions, grouped into two main themes, namely, assessing organisational data vulnerabilities and threats (during asset disposal); reviewing the application of regulatory policies, directives and frameworks for e-waste and the management of data disposal within organisations; and compliance, adherence and monitoring of defined regulatory policies, as referenced in

Appendix C. In line with easing the flow of the conversation and providing clarity around the objective of the session, the approach and structure of the interview was explained to the respondents prior to the commencement of the session, highlighting the objective, and detailing the specific themes of the topic and how these were grouped into sections to aid the flow of the session.

As indicated previously, the study utilised semi-structured interviews made up of a combination of closed and open-ended questions.

3.6 Procedure for data collection

The research study carried out semi-structured, one-on-one engagement interview sessions were conducted with the respondents, and due to Covid 19 restrictions, online interviews were conducted through the use of MS Teams sessions, as the restrictions limited the amount of face-to-face interactions.

The approached followed by the interviewer entailed informal conversation (verbal and written) with the respondents detailing the context and the purpose of the study sessions. As part of the questionnaire preparation process, the following points were considered:

I. Opening and introductory questions (general question(s) to set the respondents at ease)
II. Middle section of the questionnaire focused more on in-depth questions based on the defined topics to ascertaining responses in relation to the research

III. Lastly, the interview established if there are any further details the participant might have wished to share that might add value to the research, wrapped up and closed the session

The interviewer then proceeded to schedule formal interviews with the various respondents through MS Teams meeting sessions, in order to enable the gathering of data for the study through the use of a combination of closed and open-ended questions, which were at times, adapted to ease the flow of the conversation, based on how the respondents had responded to certain of the questions, as detailed in the research instrument.

The 12 interview sessions conducted, were completed during the period of the 18th October 2021 to the 6th December 2021 and generally took on average 37 minutes to complete. The sessions were recorded and transcribed through MS Teams, and the researcher also captured notes during the interviews. The recordings and transcriptions were then uploaded into ATLAS.ti qualitative data analysis computer software tool, for further editing, coding and analysis.

All respondents were requested to complete and sign consent forms prior to the sessions, indicating their willingness to participate in the research project, and also acknowledging and consenting to the session being recorded. Refer to Appendix A for a sample of the forms that were sent to the respondents.

3.7 Data Analysis and Interpretation

Qualitative research, as described by Nowell et al. (2017), is intended to generate knowledge grounded in human experience. Nowell et al. (2017) further went on to characterise data analysis as one of the most complex phases of qualitative

research, but the one that seems to receive the least amount of attentive discussion, however, it forms the foundational instrument for qualitative analysis. There are various approaches with specific techniques that have been identified for conducting, documenting, and evaluating, and analysing data, and in this research, the thematic analysis method was utilised, which is described by Braun and Clarke (2006) as a method used to identify, analyse, and report on specific patterns or themes that emerge from data collected. The researcher in his approach prescribed to, and followed the phases of thematic analysis, detailed by Nowell et al. (2017), below:

I. Phase 1: Familiarising yourself with your data
II. Phase 2: Generating initial codes
III. Phase 3: Searching for or identifying themes
IV. Phase 4: Reviewing themes
V. Phase 5: Defining and naming themes
VI. Phase 6: Producing the report

3.8 Limitations of the study

The key limitation of the study were that:

I. The sample size selected might not have been large enough to be representative of the population
II. Interviews were conducted through online media, as a result of the Covid 19 pandemic, which were restrictive in terms of visual and non-verbal cues which would have been more evident in a face-to-face setting, which would have otherwise aided in providing added context to the interview

III. As the sample of respondents was only targeted at a select group of senior individuals within the targeted organisations, it does not factor in the perspective of middle to lower-level staff within the respective organisations

3.9 Transferability and dependability

3.9.1 Transferability

Transferability denotes the extent to which the outcomes from research studies conducted can be applied or transferred to other individuals, and individuals that were not part of the study are able to be associated with these outcomes, thus making it generalisable (Anney, 2014). In the context of the study, transferability would relate to how organisations that were not part of the study would view and apply the outcomes of the assessment performed through a structured and standardised interview guide, assessing e-waste and data management, and the vulnerabilities to which organisations are exposed when disposing of electronic devices, when they have reached their EOL, as classified by defined organisational policies.

3.9.2 Credibility

As highlighted by Sinkovics et al. (2009), credibility is focused on bridging the gap between the realties created by the respondents in the study and those created or defined by the researcher in an attempt to draw similarities in the constructed realities. In the context of this research, the researcher, to ensure that the desired confidence and quality was obtained through the process of collection,

interpretation, and analysis; leveraged the guidance and feedback of the appointed academic supervisor and the scholastic committees to ensure credibility in the findings and through these review and ratification processes, ensured the outcomes to the questions provide a true and accurate reflection of the participants' lived experiences and perceptions.

3.9.3 Dependability

For research to achieve a level of dependability, it is expected that the researcher demonstrate that the process applied to conduct the research was done in a logical manner and documented in a way that all outcomes or events are clearly traceable (Nowell et al., 2017). According to Nowell et al. (2017), a way to achieve this is for an audit or verified examination of the research conducted, which in the instance of this study, entailed how records of all interview recordings, transcripts of the respondents' response, were logged, categorised and analysed and whether a structured and methodical approach was followed, and the evidence produced can then be verified through checks to determine if a logical and systematic approach was followed.

3.10 Ethical considerations

The research prescribed to all ethical research standards as defined by the University of the Witwatersrand, and was only conducted once approval was obtained from the ethics committee based on stipulated requirements to complete the research as detailed in Appendix E.

The researcher at all times ensured that:

I. All respondents were requested to complete and sign consent forms prior to the sessions, indicating their willingness to participate in the research project, and also acknowledging and consenting to the session being recorded, as referenced in Appendix A

II. All respondents prior to the session were sent communication detailing the context and the purpose of the study, and outlining the proceedings of the interview sessions

III. The respondents and the institutions that they are employed by were not identified in the result (unique identifiers, for example Respondent 1-n were utilised) in order to maintain confidentiality

IV. All parties involved in the research and their identities, and that of their respective organisations at all times, are to be protected

V. Nobody was discriminated against at any stage of the research, and that in no way were any threats created or any people adversely impacted in their physical environment

4 PRESENTATION OF RESULTS

4.1 Introduction

In this chapter, the findings from the research conducted were analysed, outlining the findings of the study through the methods and techniques detailed in the Research methodology section of Chapter 3. The research questioning assessed how data (both personal and sensitive) is managed within private sector organisations and public sector institutions when disposing of electronic ICT equipment, when these devices have reached their EOL.

The 12 respondents interviewed for the research were chosen based on the selection approach as denoted in Chapter 3, which were executives (CIO/CSO), a deputy CSO, data and security Department Heads, and infrastructure, data and security Senior Managers within institutions in the financial services sector; Director of IT security and Head of Departments for Infrastructure and security management within the government institutions and State-Owned Enterprises (SOE's); and the CEO and owner of the e-waste recycling companies situated in the Gauteng province in South Africa, were the primary sources of data collection and played a vital role in the drawing out of information and the theme creation process. As highlighted in previous chapters, the interviews were one-on-one sessions conducted utilising digital media platforms.

The findings were organised in accordance with the research propositions and formulated theoretical framework detailed in Chapter 2. Each of the sub-aims identified were linked to the applicable propositions, and the corresponding

results presented in accordance with the themes deduced from the questions posed in the research instrument.

The initial code input into ATLAS.ti was categorised based on emerging themes from the questions detailed in the research instrument. The approach was to work through the transcripts, and based on various responses from the respondents, link these to the respective codes that were formulated and identify themes that developed from the analysis. Annexures D1 and D2 provide a view of the approach followed to create the groupings.

The results from the data collected were presented in a predominantly narrative format, with some illustrative formats used to enhance the presentation. The quotations utilised were extracted from the various interview transcripts and were captured as close to verbatim as possible, however in most instances, the filler phrases were removed to make the quotations clearer, and easy to follow. In certain instances, statements with similar context or explanation were paraphrased to give a collective view point of the respondents' thoughts.

4.2 Results pertaining to vulnerabilities, data management and data classification

In this section, the results related to the findings collected from the interview session are presented. Here we assess all the findings that pertain to our first proposition. The sub-aims linked to the first proposition, guided by the research questions, associated to these sub-aims form the basis for this session of results presentation, and allow the researcher to further unpack the associated themes that have emerged from the patterns discovered from the developed code during

the data analysis process, Figure 3 below provides an illustrative representation of this breakdown.

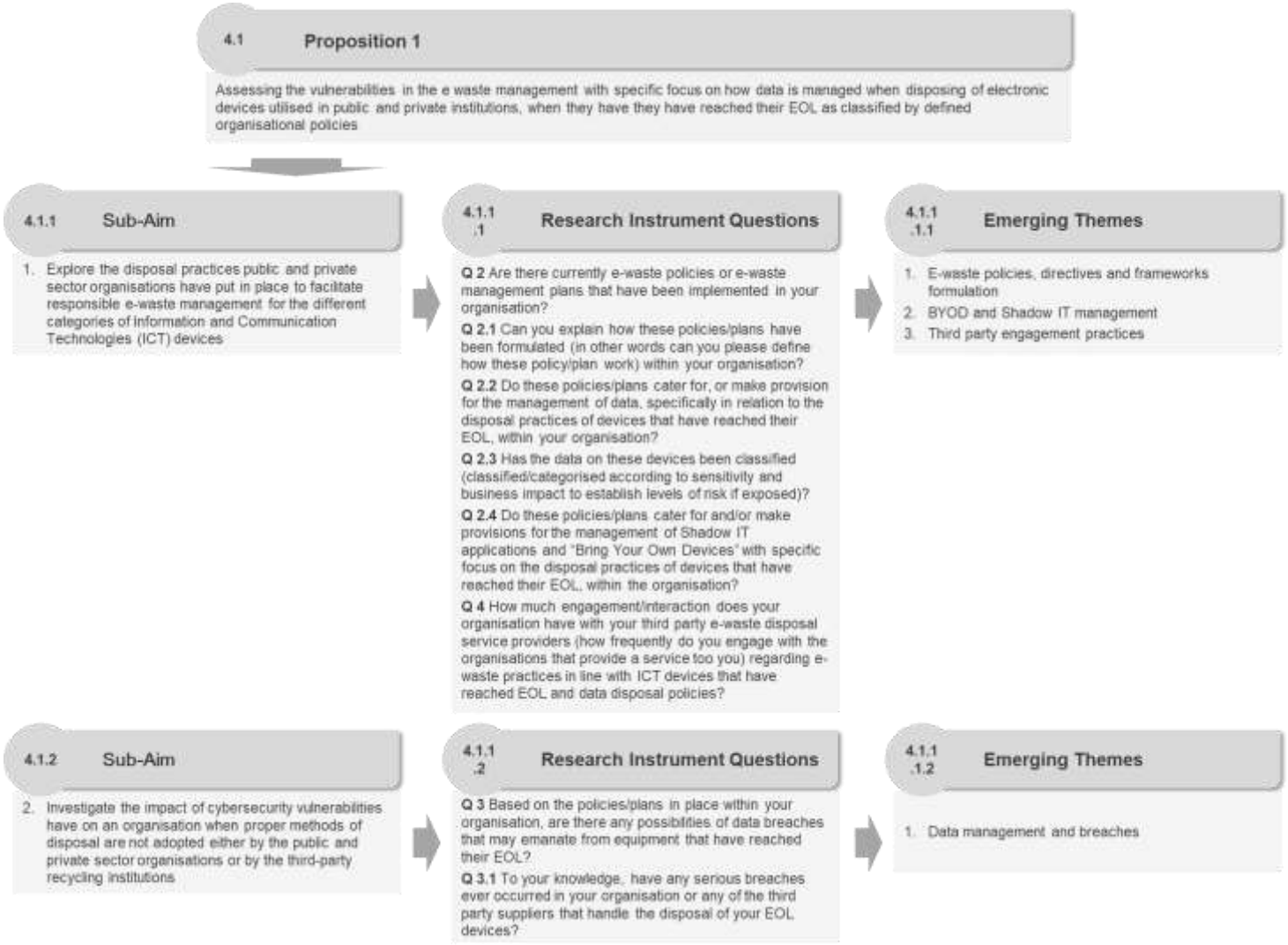


Figure 3: Research process association between proposition, sub-aim, instrument questions and emerging themes (part 1)

4.2.1 Organisational disposal practices to facilitate responsible e-waste management

The findings of the study were based on the analysis of the data obtained from the interview respondents. This section focused predominantly on various asset

and data disposal practices and guidelines that have been set up in the various organisations. The key task was to try and ascertain from the respondents how the various regulatory policies, directives and frameworks for e-waste are applied; and linked to this, how these are managed within their respective organisations.

I. E-waste policy development and implementation

To address how e-waste policies have been developed and implemented within the various organisations, we assess how respondents addressed and responded to the three main questions that focused on this topic which were:

Q 2 Are there currently e-waste policies or e-waste management plans that have been implemented in your organisation?

Q 2.1 Can you explain how these policies have been formulated (in other words can you please define how these policies work) within your organisation?

Q 2.2 Do these policies/plans cater for, or make provision for the management of data, specifically in relation to the disposal practices of devices that have reached their EOL, within your organisation?

Considering their awareness of policy management practices specifically around the management of devices within their organisations, respondent's provided varying views specifically from an awareness perspective, and how it is managed within the various functional areas. Of the 12 individuals interviewed, 11 of the respondents indicated that policies did exist, highlighting that in most instances, that it did not only explicitly address e-waste management as articulated by Respondent 5, but was encapsulated into their broader IT policies, although in some instances, did not cover the bare minimum around the specific

requirements, as detailed within their respective organisations and that they were aware of its contents.

“It doesn't speak directly, only to e-waste management, but in our IT policies we do have reference to e-waste” - Respondent 5.

A respondent in the public sector indicated that due to the structural changes within the organisation, they were afforded the opportunity to relook their various policies providing them the opportunity to eliminate policies that were outdated and meaningless in the current context of operation. It also allowed them to focus on policies that cater and make provision for the transition into a digitally led organisation focusing their efforts towards creating a structured framework for data and asset management, and IT security at its core. Building off this, they would have the right level of skill and process to drive execution and in turn, manage the business impact, based on an established level of risk exposure and, to support this view, it was based on the awareness that this is an area that needs to be remediated to heighten the awareness and sensitise users to the far-reaching implications e-waste has, on the environment, due to toxic contaminants generated (Mihai, 2021), coupled with the rise in energy consumption of data centres contributing emissions (Trueman, 2019) and the numerous cybersecurity related threats to which industries and societies at large could be exposed.

However, almost half of the 12 respondents highlighted that policies were implemented from a group perspective and employed a top-down approach in relation to implementation and management practices, but the implication of this is that the management practices are passed off to other functional areas and

there was no clear awareness by some of the respondents as to the process that gets executed in these areas.

“It's is managed by the group itself and not and not by merchant solutions. So we obviously reporting to the group, into their standards. So yes, definitely” - Respondent 4.

II. BYOD and Shadow IT policy management

To address how organisations define BYOD and Shadow IT as the various ways organisation and the employees within these organisations are making use of these technological benefits, and they view these key components that could have a potential bearing on how devices are managed when devices have reached their EOL and have transitioned into the disposal phases, we looked at the response to the question:

Q 2.4 Do these policies cater for and make provisions for the management of Shadow IT applications and “Bring Your Own Devices” with specific focus on the disposal practices of devices that have reached their EOL, within the organisation?

From the respondents’ engagements, it was ascertained that organisations had varying approaches to BYOD and shadow IT management, nine of organisations did allow for and made provision for BYOD, and accommodated the use of shadow IT software and applications services for remote usage, however to enable this, individuals needed to prescribe to the various device management and IT security polices, that would ensure that data is secure and properly managed over the organisations’ network, also ensuring all the data on that

device is properly wiped off when devices are lost, stolen or has reached its EOL, this was well articulated by Respondent 7.

“So from a, Bring Your Own Devices that is accommodated for, we've got the device management policy and it stipulates that if anything happens to your device whether it's your laptop, your own personal laptop or your mobile phone, then everything must be encrypted and if you lose that that that laptop or that device then it will be wiped off. All the data on that device will be wiped off.” - Respondent 7.

Two of the respondents, specifically in the financial services sector, indicated that their organisations did not cater for BYOD and shadow IT application services and that all devices and software applications that were utilised for business operation purposes were supplied by the organisations’ IT department, this was to try and minimise the security risks of devices that have not been adequately encrypted having access to the networks.

“So we don't allow bring your own devices into our corporate network. We do have wireless networks where you can connect a personal device too, but then you have a straight connection to the Internet, so we do not support bring your own devices.” - Respondent 3

Only one of the respondents indicated that they were not particularly sure about the policy and its specifics as it did not relate to his executable functions but, based on his opinion, the functional area responsible for BYOD would ensure that all devices utilised prescribed to all security requirements and that the data accessed and utilised on these devices were done in a safe and secure manner with nobody being able to access the data.

III. Third-party engagement impact on policy formulation

From a third-party engagement perspective, we focused on ascertaining how the engagements between the various parties within the value chain could influence the formulation of policy looking at the question:

Q 4 How much engagement or interaction does your organisation have with your third-party e-waste disposal service providers (how frequently do you engage with the organisations that provide a service to you) regarding e-waste practices in line with ICT devices that have reached EOL and data disposal policies?

With respect to third-party engagements, almost all respondents indicated that there was some form of engagement or interaction with their third-party suppliers. Three of the respondents, specifically in the private sector, highlighted that most engagements stemmed from a contractual execution perspective and that they had frequent and on-going engagements, however what was noted is that there were opportunities to utilise these engagement platforms more effectively. This would contribute to a two-way improvement cycle in terms of threats that arise and joint efforts to put policies and frameworks in place to jointly try and mitigate them. One respondent within the financial service sector proposed that there be a review of their strategic approach and look at the specific pros and cons of insourcing and outsourcing of the physical disposal of assets with the specific focus on data management, given the type of data they deal with and the associated risks that could emanate from any potential leakages or breaches.

4.2.2 The impact of cybercrimes on an organisation when proper of disposal methods are not adopted

This section of the discussion focused on understanding, based on the policy frameworks that have been put in place within the organisations, what some of the elements that may emanate that could create the possibility of data breaches, from equipment that has reached their EOL. As indicated in the previous section, one of the key driving factors was to try and ascertain from the respondents what have been some of the failing points in their processes that may have resulted in a breach and when did these breaches occur.

I. Data management and disposal practices

Through the research instruments, we posed two questions which predominantly focused on any inherent gaps or vulnerabilities in the policies that could result in a data breach based on respondents' insights and experience, and their awareness of any such breach having occurred. For this section, we placed more focus on the question related to the vulnerabilities which was posed as:

Q 3 Based on the policies in place within your organisation, are there any possibilities of data breaches that may emanate from equipment that has reached their EOL?

What was common from the responses provided by the respondents was that there had been no real awareness or indication of breaches that were as a result of gaps or vulnerabilities in the disposal practices, but also, breaches that emanated were from cyber related threat vectors.

However, a sentiment shared by four of the respondents is that due to the rapid evolution of the technological landscape, nothing is ever guaranteed and that they should never become complacent in their actions, as articulated by Respondent 5.

“I will never tell you there's no risk of a data breach due to something right? It's an evolving world. But I think it is something that we should actually be worried about. Of course, I remember, when you know what, people call it dumpster diving, right? Where they go through all the paper documents to try and reassemble information. I mean computer is designed to retain information. So it is a natural thing too. If you want to go and do dumpster diving, that's a place to go. You know your waste is a different source.” - Respondent 5.

4.3 Results pertaining to driving organisational compliance through policy enforcement

In this, the second part of the section, we assess all the findings that pertain to our second proposition. The sub-aims linked to the second proposition, guided by the research questions, associated to these sub-aims which form the basis for this session of results presentation, and allow the researcher to further unpack the associated themes that were applied to the influence of government in guiding organisations to define and develop regulatory policies, directives, and frameworks for e-waste and how these should be managed within organisations. Further to this, we try to understand the level of compliance, adherence, and monitoring of defined and implemented policies and governance frameworks

employed within the organisation and the way these are assessed, and awareness and training managed and facilitated within organisations.

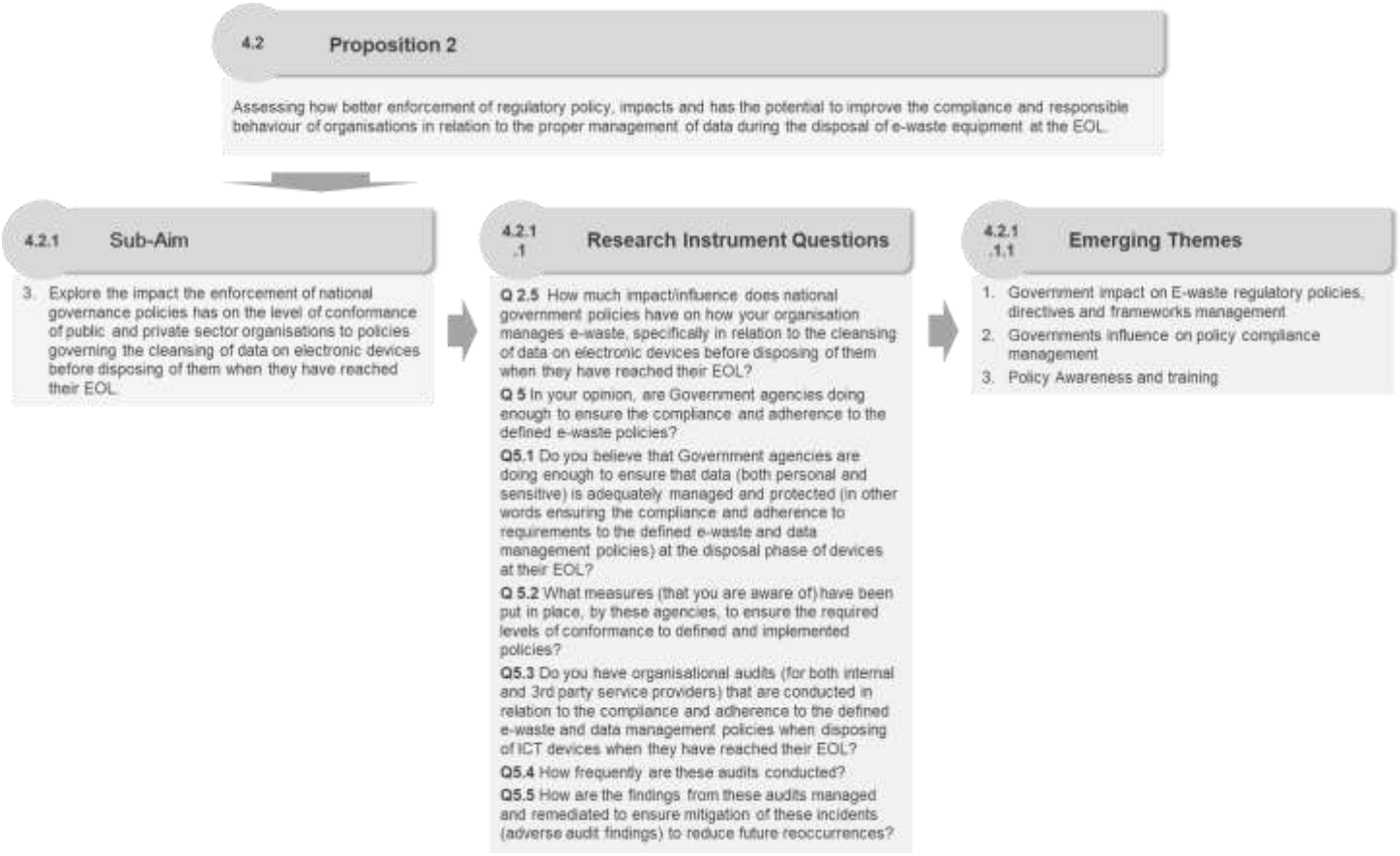


Figure 4: Research process association between proposition, sub-aim, instrument questions and emerging themes (part 2)

4.3.1 The impact national governance policy enforcement has on organisational conformance practices

From an organisational perspective we sought to understand the level of government influence and the way the organisation has defined and presented its respective policy frameworks and what procedures have been put in place to ensure that a sufficient level of training, and awareness measures have been established with regard to the respective policies, and to understand the impact

the degree of ease of implementation could have on how individuals interact, manage and adhere to cybersecurity and data management requirements in relation to the utilisation practices of their devices and more importantly, how they manage the disposal of electronic devices when they have reached their economic EOL within the organisation.

I. Government impact on e-waste regulatory policies, directives, and frameworks management

To address government's impact and influence on how e-waste policies, directives and frameworks have been used as a baseline, and input into the formulation and implementation of policies within the various organisations, we assess how respondents addressed and responded to the question that focused on this topic, which was:

Q 2.5 How much impact or influence do national government policies have on how your organisation manages e-waste, specifically in relation to the cleansing of data on electronic devices before disposing of them when they have reached their EOL?

A sentiment displayed by four of the respondents indicated although various policies and frameworks have been formulated, these have prescribed predominantly around waste management, however more needs to be done to ensure that there are clearer and more prescriptive directives around e-waste and data management of electronic devices. Equally important, based on what was highlighted by the respondents, is the role government needs to play in ensuring that these policies are translated into implementable and sustainable standards, and that all parties within the ecosystem should be held accountable

for ensuring that these are actioned within their respective environments. This was well articulated by Respondent 11 when he said:

“So up until up until very recently there was no legislation specifically written for e-waste, so if you take care even national environmental Waste Management Act, doesn't specifically refer to e-waste, so it's only now come the 5th of May of this year with the extended producer responsibility organization where there's specific reference to handling of e-waste. However, the regulations were published, but the standards weren't published. So as we speak right now, there's no official government standard on the handling of e-waste, and that's something that there is a task team of which we indirectly involved in it is busy developing this, but it could be another two years before there that become comes out as an industry standard”. - Respondent 11.

Five of the respondents shared a different opinion, as they highlighted that in their opinion, government did not really play a big enough role or did not have much or any influence on how policies are managed, as in their opinion, they had a better grasp as to what e-waste management constituted than the government, and to some extent, that the frameworks they had in place were more detailed and robust than what was being prescribed by government, and this was in part because they had better knowledge in this specific subject matter.

II. Governments influence on managing policy compliance

Having sought to understand government’s impact and influence on how e-waste policies, directives and frameworks have been used in organisational policy formulation, we look further at the government level of influence in ensuring the correct level of compliance to the defined policies and ensuring that the various

institutions conform to these legislative directives; we assess how respondents addressed and responded to the question that focused on this topic which was:

Q 5 In your opinion, are Government agencies doing enough to ensure the compliance and adherence to the defined e-waste policies?

Q5.1 Do you believe that Government agencies are doing enough to ensure that data (both personal and sensitive) is adequately managed and protected (in other words ensuring the compliance and adherence to requirements to the defined e-waste and data management policies) at the disposal phase of devices at their EOL?

Q 5.2 What measures (that you are aware of) have been put in place, by these agencies, to ensure the required levels of conformance to defined and implemented policies?

Respondents from all sectors shared different opinions with regards to the level of influence government regulatory policy has in the way the organisation has defined and presented their respective internal policy and frameworks and what procedures have been put in place to ensure conformance to these defined policies. Eight of respondents indicated that there was enough involvement from government and that they were doing enough through their interventions to ensure that organisations are compliant. Respondent 11 went as far as to indicate that industry role players should take on a larger role in the policy directives and should be playing a greater support function to government as they are at the centre and have great institutional knowledge, as indicated in his views below:

“I mean that you know it’s a good point to debate which we haven't got the time for. You know there is a limit to what government can and can't do you know? We all know the view about Big Brother and so forth. So for me this is the role that should be an industry driven role because if I'm a maker of devices that can carry data like cell phones, laptops, servers, whatever. The media is, that's beside the point, they that that's the biggest factors in my view, should sit with them so that they must be providing guidance, and these are dudes in that because they know the software they know their vulnerabilities and so therefore the ownership should be on them to ensure that they either work through industry bodies and the system and train specialists who can go out and advise”. - Respondent 11.

Two respondents indicated that they did not believe there was enough involvement from government and that they were doing enough through their interventions to ensure that organisations are compliant, with two other respondents opting not to comment.

“So that's what I think, in terms of, the higher technical side to that there's nothing much done by government. But I think the impact of government comes with elements where the environmental aspects cause the world has its eyes on the environmental issues.” - Respondent 6

Added to this, three of the respondents from the e-waste disposal management and financial services sectors further indicated that they believed that government needs to put in place more distinct policies and mechanisms to measure overall organisational conformance to regulatory policy and how non-conformance is managed, specifically in the area of e-waste, as there has not really been specific policy that focuses predominately on this topic.

An area that was further raised by two of the respondents, that was of concern, was centred around the waste (dumpster diving) and scrapyard (landfill) collecting of electronic waste and the hazardous dismantling practices, without the use of the appropriate tools by the waste pickers in their attempt to access the valuable items or components for financial remuneration, and what measures could be put in place to manage this area, not only by creating more structured environments for these individuals to be able to work in, but also facilitating these individuals being able to learn more about the value chain and the associated policies aligned to the process and what role they could play in ensuring conformance to these standards.

III. Policy Awareness and training interventions

A point that came out quite strongly, specifically from six respondents from the private sector respondents, but a sentiment echoed by one of the respondents from the e-waste disposal sector was that, in relation to both conformance to regulatory and internal organisational policy was the component of awareness and training in that respondents alluded to the fact that this was a pivotal area in how these are implemented and practised, specifically around data management and disposal practices in organisations, ensuring the right level of compliance and conformance to any implemented policy. The following comment is detailed by Respondent 3 on the key views around awareness, a sentiment that was echoed by the other respondents:

“I think there needs to be more awareness made. You know that when you sell a device you know you can go delete your files etc. People don't understand that the data is still recoverable. There's very basic understanding of this. So yes, I

think awareness is something we underplay a lot we need to do more awareness about how to protect and what to protect. I think people don't realise”. - Respondent 3.

4.4 Summary of the results/findings

The findings from the analysed data highlighted a couple of factors that, based on the views from the Respondents, would prove pivotal in the uncovering the themes that would emerge from the findings.

We assessed all the findings that were linked to our first and second propositions. The sub-aims linked to the respective propositions, guided by the research questions, and associated to the sub-aims formed the basis for the details of the results derived from the various interview sessions. This allowed the researcher to further unpack the associated themes that would have emerged and the patterns that were uncovered from the code developed during the data analysis process.

Some of the key elements that were focused on and derived from the responses related to:

I. How the various regulatory policies, directives and frameworks for e-waste are applied; and linked to this, how these were managed within their respective organisations, looking at aspects pertaining to
    a. The various mechanisms that have been put in place to measure overall organisational conformance to regulatory policy and how non-conformance is managed,
    b. Conformance to regulatory and internal policy and the level of awareness and training created to ensure compliance and conformance to implemented policy,

II. Data management practices, specifically around the management of EOL devices within their organisations and how these policies have been defined,

III. How organisations define BYOD and Shadow IT as the way organisation and the employees within these organisations make use of these technological benefits, view these key components that could have a potential bearing on how devices are managed when devices have reached their EOL and have transitioned into the disposal phases,

IV. Third-party engagement practices and the various improvement and enhancement opportunities that could be derived from ongoing engagements,

V. The various breaches that have occurred in several organisations, specifically relating to cyber related threat vectors for devices that have been disposed of after reaching their EOL,

VI. Government's influence and the way the organisations have defined and presented their respective policy frameworks and what procedures have been put in place to ensure that an adequate level of training and awareness measures have been established with regards to the respective policies detailing

    a. The various mechanisms that have been put in place to measure overall organisational conformance to regulatory policy and how non-conformance is managed,
    b. Conformance to regulatory and internal policy and the level of awareness and training created to ensure compliance and conformance to implemented policy.

In the next Chapter we discuss and unpack in detail the findings derived from the various respondents and bring in various literature presented in Chapter 2.

5 DISCUSSION OF THE RESULTS OR FINDINGS

5.1 Introduction

This chapter analyses the key findings that emerged from the study. It assesses the vulnerabilities organisations, specifically financial and government institutions, are exposed to and interrogates the management policies and operations for managing the disposal of e-waste at the end of asset life cycle, specifically in respect of data.

The constructs defined in UTAUT2, and components, both internal and external to the organisation, detailed in the cyber-defence framework, serve as key contributing factors for the analysis. The study focuses on the constructs that are directly interrelated to the various regulatory policies, directives and frameworks for e-waste and how they are applied and managed within the respective organisational settings. The key focus is on the various asset and data disposal practices and guidelines that have been set up within these organisations and the various cybersecurity related threats they may be exposed to when these devices have reached their respective EOL.

5.2 Vulnerabilities and data management policies

This study assesses vulnerabilities in e-waste management policies, in financial and government institutions with a specific focus on how data is managed when disposing of electronic devices that have reached their EOL.

5.2.1 Device disposal practices and data management

From the data, it emerges that device disposal practices (DDP) are largely formalised in most organisations with well-defined policies, processes and procedures governing the treatment of devices when they have reached their EOL. These generally focus on the classification, retrieval, cleansing, shipping, and disposal of these devices. However, some organisations have informal DDP, where devices that have reached their EOL are stored, but are not formally tracked and managed. Ichikowitz and Hattingh (2020) support these findings around the prolonged periods that EOL devices are often stored. They further state that the management of electric and electronic equipment can be categorised into interdependent actions, which is managed from the point that they are retrieved for disposal, up to the point where they have been dismantled and discarded.

These devices that often contain PII could have dire ramifications for the organisation if they fall into the wrong hands, and the PII is accessed through various retrieval methods. This can be illustrated in PII breaches like the Equifax data breach where cyber attackers, were able to access the PII of over 143 million customers belonging to Equifax, due to a flaw in one of their applications (Wattles & Larson, 2017). Another example is the case of Liberty Life, where through a breach in its email repository, the PII of over 30 million clients was accessed and a ransom requested (IOL, 2019). In order to curb this rise in PII breaches and enforce compliance with POPIA, the information regulator currently imposes a fine of up to R10 million for any violations (DLAPiper, 2021).

Alghazo et al. (2018) highlight that more awareness needs to be created regarding data privacy, focusing attention on EOL devices and mechanisms to ensure the correct levels of protection are put in place to secure data throughout the various phases of the disposal value chain.

This directly addresses the element of data management on EOL equipment which emerged from the data and is a critical layer in DDP policies. These policies prescribe a systematic approach for the removal of PII and any data that is deemed to be of a sensitive nature from these devices and ensure that there is no way that the data can be recreated and utilised for malicious intent.

5.2.2 Device disposal and cyber attacks

It was reported that there were no cyber-attacks attributed to information extracted from EOL devices incorrectly disposed of. Attacks identified were via traditional attack vectors like compromised or stolen credentials, ransomware, phishing, and missing or poor encryption, to name a few. However, what also emerged is that little emphasis is placed on what happens to data once a device no longer has a meaningful purpose and has reached its EOL. Forgor et al. (2019) state that the majority of people are unaware that electronic devices that are discarded potentially contain some levels of PII that can be accessed through various retrieval methods by individuals with malicious intentions.

I. E-waste management

There was a shared acknowledgement by some of the respondents that more focus and analysis was required by organisations, in relation to e-waste management and how data is managed on devices at EOL. Forgor et al. (2019)

support this, indicating that data security from e-waste is an area of concern as most users do not employ the correct techniques to discard their PII; this in turn, creates security vulnerability to which many individuals are oblivious. This could be attributed to the fact of individuals' belief that the standard security features on devices are secure enough, and that no additional measures are required to ensure that their PII is not accessible when being discarded (Alqahtani & Braun, 2021; Escobar-Rodríguez & Carvajal-Trujillo, 2014).

Debnath et al. (2019) and Thing and Tan (2012) add to this argument by bringing in the element related to the various mechanisms used for retrieving PII from EOL devices, with emphasis placed on reverse engineering techniques that could be employed by criminals to exploit and use to their benefit the security vulnerabilities of these electronic devices.

This draws to the eight essential conditions, as defined in POPIA, detailing how organisations and their third-party suppliers handling and managing PII must apply in order to ensure compliance with the effective protection of this information (Adams et al., 2021). This places the onus on the organisation to define policies with well documented processes and procedures that prescribe to the correct destruction and disposal practices for all devices and the PII and sensitive information contained on them, in a manner that prevents any reconstruction and unauthorised access during disposal (Schepers & Novazi, 2020).

Coupled to this, Schepers and Novazi (2020) highlight that it is imperative for organisations that have sought the services of third-party suppliers to manage the destruction of their data or devices, ensure that these service providers have

policies and standards that comply to POPIA. Ultimately, both institutions remain liable for any breaches that may occur, according to the act, but the organisation that sought the service still remains accountable (Adams et al., 2021).

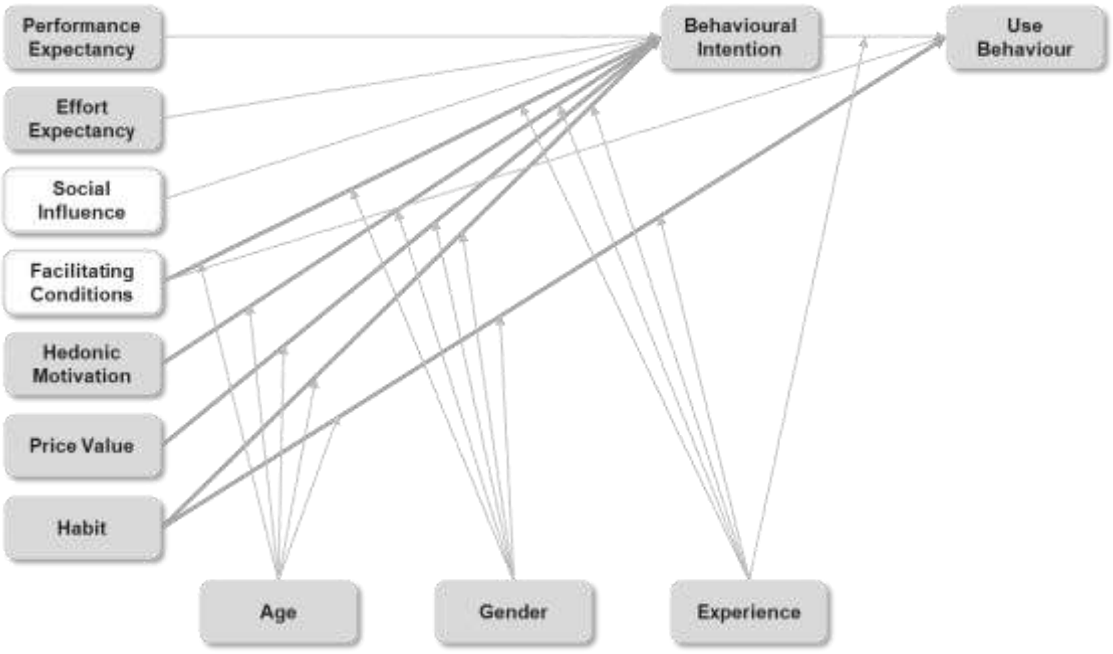


Figure 5: UTAUT2 Model (Alqahtani & Braun, 2021) – Social Influence and Facilitating Conditions Constructs applied to analysis

When factoring in the Facilitating Conditions construct of UTUAT2 highlighted in Figure 5, we look at the aspect of how individuals are over-reliant on systems and mechanisms that have been put in place by the organisations and the device producer, without understanding the implications in relation to not adding additional security features and prescribing effective mechanisms to drive efficient device disposal and data management practices.

Additionally, we can factor in the construct of Social Influence as highlighted in Figure 5, based on the awareness created and derived by how individuals will view certain of their actions (Kan & Fabrigar, 2017). This can be linked to how the opinions of people within individual close networks have an impact on how

they behave, based on their perceived understanding and experience of the set topics. This is then associated with e-waste management practices, and how their subsequent actions related to conformance and non-conformance to policies. Ultimately, this impacts on how these individuals prescribe to effective data management and cleansing practices.

5.2.3 BYOD and Shadow IT policy management

Nine of the 12 organisations made provisions for BYOD and the use of shadow IT software in their operational environment with varying approaches. Where BYOD was allowed, employees were required to prescribe to the various device management and IT security polices to protect PII and sensitive corporate data. The policies ensured that PII is properly erased from devices when they reach their EOL.

Donaldson et al. (2015, p. 43), agree with this argument, detailing that the lack of adequately formulated organisational policies often exposes organisations to various BYOD, shadow IT application services and other cybersecurity related risks. It is in this vein that organisations need to ensure that they implement the necessary security measures, coupled with policies to avoid leakage of company data while still abiding by all data privacy laws (Veljkovic & Budree, 2019).

However, the key to this is employees' understanding and interpretation of these policies, how they practice these policies and a clear appreciation of the implications if the organisation is exposed to BYOD, shadow IT application services and various cybersecurity related breaches due to the non-

conformance and negligence. This is a notion supported by Veljkovic and Budree (2019) and Downer and Bhattacharya (2015) who point out that the success of effectively compiled and implemented policies relies heavily on user awareness and education which stems from an organisational need for employees to play a more substantive role in the general cybersecurity enforcement.

A differing view that emerged from our study indicates that certain organisations do not cater for BYOD or shadow IT application services. All devices and software applications that are utilised for business operations are supplied by the organisation. This is to try and minimise cybersecurity risks related to devices' disposal management and the unauthorised access to the organisations IT networks. This could be attributed to these organisations seeking to limit the accountability burden on their employees misinterpreting or misunderstanding policies which could have a negative impact on the organisation.

Chigada and Daniels (2021) indicate that due to the lack of proper protective mechanisms, BYOD has the prospect to adversely affect an organisation's security systems and infrastructure. Even though organisations have well defined policies related to BYOD, the challenge they face is predominately the management of employees (Chigada & Daniels, 2021). This is supported by Cho and Ip (2017), who indicate that due to the complexities around BYOD and employee conformance, organisations prescribe to the approach of corporate owned devices, which can securely be utilised by employees for both work and personal purposes.

This can be tied into the Habit construct of UTUAT2 detailed in Figure 6 below, focusing on the execution of BYOD and shadow IT application policies and how these influence the individual's habitual practices and how the automatic execution of certain activities or functions impact positively or negatively on the level of conformance to what has been prescribed by the data management and device disposal practices.

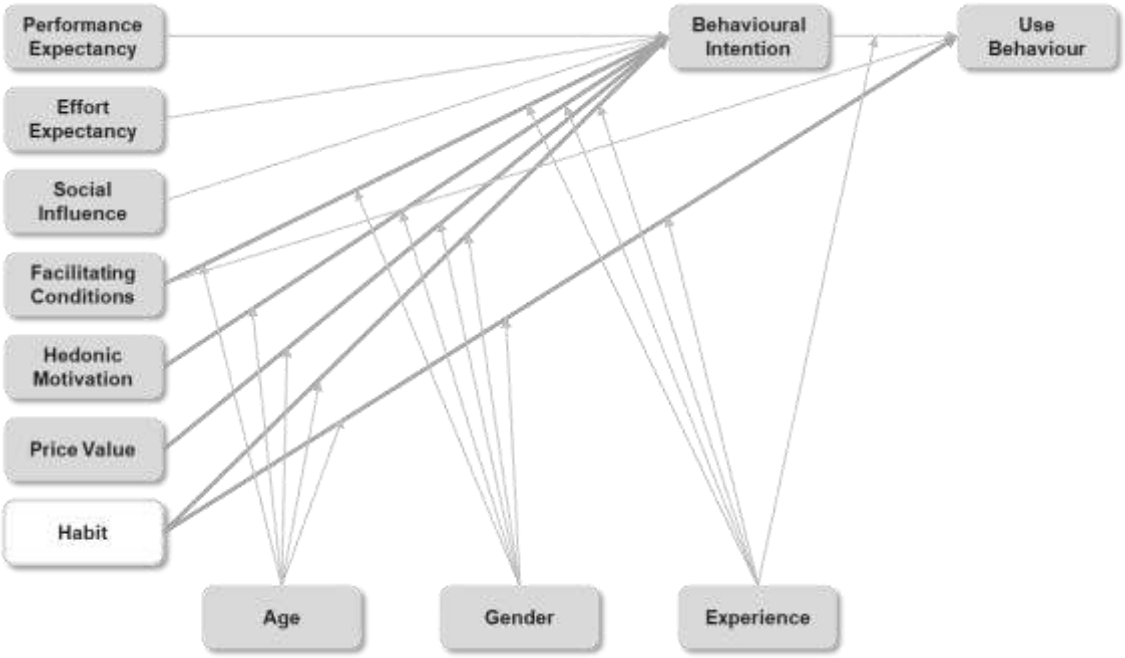


Figure 6: UTAUT2 Model (Alqahtani & Braun, 2021) – Habit Construct applied to analysis

5.2.4 Data vulnerabilities in extended supply chains

When considering third-party suppliers and the inherent risk of exposure of data on disposed of ICT devices, the responsibility sits with the organisation to try to understand the level of commitment to the formulation of solid and robust processes and procedures. These need to be aligned to defined organisational policies and facilitate effective engagement practices among the various

respondents within the supply value chain to drive the assurance that suppliers meet the needs of their clients. This, in turn, will facilitate operational activities that ensure all inherent risks are mitigated and a good reputation is maintained for all parties involved (Jones, 2009).

I. Third-party EOL management

Eight of 12 organisations employ third parties for EOL management. Most engagements stem from a contractual execution perspective on the setting up and managing of the defined DDP agreements. Our data highlighted the need for all parties to come together to ensure that the correct level of accountability is placed at the right stages of the value chain, and all parties take the responsibility to ensure that the correct level of implantation, awareness and training is created to ensure all e-waste is managed according to the appropriately defined standards. The responsibility for an effective echo system needs to take all individuals or industry role players into consideration and all should have a vested interest and take on a more substantial role in setting policy directives and driving regulatory compliance.

Organisations, through the application of the correct level of due diligence, with robust screening mechanisms and continual monitoring of their disposal partners, could address this by ensuring information security, proper disposal practices, and regulatory compliance are key factors during their third-party partner selection process (Warner et al., 2012, p. 13). This is supported by Marks (2011), who adds that effective ITAM and ITAD plans are reliant on a well-established chain of custody, defined as a faultless chain of evidence, supplied by asset disposal partners detailing the exact process and procedures followed to dispose

of IT assets, with a clear audit trail and built in deterrence mechanisms to reduce risk of theft or loss, due to negligence.

Further to this, a point that emerged from the data is that from a strategic leadership view, critical consideration should be given to the specific pros and cons of insourcing versus outsourcing of the disposal of their assets and electronic devices, with specific focus on data management, and given the type of data with which they deal.

Warner et al. (2012, p. 11) support this notion highlighting that, as part of formulating a secure corporate ITAD plan, that organisations assess the feasibility of either in-house or third-party disposal. This decision will be guided by how the organisation is able to justify the capital expenditure for either route, ultimately contributing to the most feasible and cost effective approach (Warner et al., 2012, p. 11).

5.3 Driving organisational compliance through regulatory policy enforcement

This part of the study assesses how enhanced enforcement of regulatory policy has the potential to improve the compliance and responsible behaviour of organisations in relation to the proper management of data during the disposal of e-waste equipment at the EOL.

5.3.1 Formulating regulatory policy frameworks and managing compliance

With respect to national legislation and regulations, our study reveals a mixed set of views regarding the formulation of regulatory policy, and the level of influence this has on the way the organisations have defined and implemented their respective organisational policies and frameworks, and the various procedures that have been put in place to ensure compliance to these defined policies.

It is important to note that in the current South African landscape, there are no specific legislation that explicitly focuses on e-waste (Finlay, 2007). E-waste in South Africa, is included in the Waste Act, 2008 (Act No. 59 of 2008), and currently governed by 13 pieces of legislative acts. These as detailed in (SAWIC, n.d) which include:

I. The South African Constitution (Act 108 of 1996)
II. Hazardous Substances Act (Act 5 of 1973)
III. Health Act (Act 63 of 1977)
IV. Environment Conservation Act (Act 73 of 1989)
V. Occupational Health and Safety Act (Act 85 of 1993)
VI. National Water Act (Act 36 of 1998)
VII. The National Environmental Management Act (Act 107 of 1998)
VIII. Municipal Structures Act (Act 117 of 1998)
IX. Municipal Systems Act (Act 32 of 2000)
X. Mineral and Petroleum Resources Development Act (Act 28 of 2002)
XI. Air Quality Act (Act 39 of 2004)
XII. National Environmental Management: Waste Act, 2008 (Act 59 of 2008)

XIII. National Environmental Management: Waste Amendment Act, 2014 (Act 26 of 2014

As highlighted by Sovacool (2019) policies, legislation and regulations developed and put in place at a national level need to be put into action, and should not just exist as documented policies on paper only. Based on this it is vital for organisations to take these emergent frameworks, and develop robust organisational level policies that will drive operational level compliance.

Borthakur (2020) further adds that it is imperative that these policy efforts are constantly reviewed and re-assessed at regular intervals to identify possible gaps in implementation, to ensure interventions are put in place to maximise the potential for compliance. This is supported by the views of Alqahtani and Braun (2021) who argue that compliance to policies does not only refer to a reactive response due to changes in behaviour, conduct, and attitude of individuals, but should be viewed as a continuous process that is constantly evolving and is aligned to defined goals or objectives.

I. Government impact on e-waste regulatory policies management

It is government's responsibility to ensure that they set policy directives. However, it is equally important for the industry role players and practitioners to provide insights and suggestions to ensure these policies are implementable and sustainable, and all parties should be held accountable for the respective roles they play in this ecosystem. This was a sentiment that was echoed and supported by respondents, derived from our data, which confirms the fact that for effective and sustainable policies to be developed, implemented and managed, it is the responsibility of all role players to play their part.

Sovacool (2019) acknowledged that there is an inherent need for further formalisation and more stringent policy measures to be implemented within the e-waste sector. This needs to be supported by the involvement of the private sector actors who could be key in terms of driving the formalisation of policy directives, given their knowledge, experience, and expertise related to waste and e-waste management processes (Sovacool, 2019).

Maphosa et al. (2020) adds to this, highlighting that over the years, there has been a steady increase in intra-African e-waste movement from various countries, specifically those with porous borders due to the financial gains earned from these recycled goods. This addresses the concerns around the effective implementation and management of e-waste regulatory policies.

With policies and regulations which are not effectively governed and managed, criminals could be presented with opportunities to exploit these gaps for their illicit gains. This indicates that government needs to be more focused and targeted with regards to e-waste policies Maphosa et al. (2020), and need to appreciate the complexity of the various e-waste and data management streams. Based on the various facets within these streams, there is a need to create a framework that addresses each of the components on their merit, which culminates into an integrated e-waste and data management policy, providing directives in the management of e-waste and data for all devices from cradle to grave.

This is further supported by the views of Ameen et al. (2021), who denotes that organisational cybersecurity will not improve unless all parties in the ecosystem start forming working synergies and utilising the inputs of the various industry

technical security experts to improve the collective understanding of security difficulties and define the critical tools required to address these issues.

II. Governments influence on managing policy compliance

From the data, it emerged that there is an appreciation that there is enough involvement from government in relation to managing the way the organisations have defined and implemented their respective organisational policies and frameworks, and that they are doing enough through their interventions to ensure that organisations are compliant.

Sabillon et al. (2016) highlight that generally, policies are instruments established by government to provide a platform for their institutions to communicate and express the specific elements that they want to manage and protect through defined regulations. Ghosh et al. (2016) add that for any policy to be effective and drive the right level of compliance, it is imperative that the management of policies are correctly understood and interpreted by the various governmental structures, thus enabling them to drive cohesive policy enforcement.

Supplementary to this is the perspective emerging from the data which focuses on the fact that it is not only government's responsibility to drive the enforcement of policy directives, but that industry role players should be playing a bigger role in supporting and driving these initiatives as they are at the centre and have great institutional knowledge.

Ikhlayel (2018) supports this notion, underlining the fact that government's function is to develop legislation that defines effective ways of managing e-waste. The directives set by government policies need to drive the enforcement of e-

waste regulations, but for proper e-waste management to be sustainable, integrative engagement and solutioning from all stakeholders involved in the ecosystem is required (Ikhlayel, 2018).

An extension of the previous view that comes to the fore is that government needs to be playing a more influential role in the governance of e-waste management, specifically in the informal e-waste sector. The sentiment shared by the respondents was that through various gaps in the regulatory environment, people are able to by-pass the various system put in place. This is resulting in non-participation in formal policy directives and ultimately, non-conformance to the regulatory policy structures.

Borthakur (2020) denotes that there in an acknowledgment that the current legislation around e-waste poses some gaps surrounding the implantation and monitoring of the sector to facilitate a sustainable e-waste management environment. Sari et al. (2021) indicate that legislation is a key determinant of driving successful policy implementation in organisations, and because of these respective laws, government has the capabilities to enforce proper disposal practices and drive a behaviour of compliance in the industry.

Alqahtani and Braun (2021) note that to enable effective cybersecurity compliance practices and drive human acceptance of cybersecurity technologies, it is imperative that all critical factors that contribute to the component of compliance and implementation are effectively identified and analysed. A compliance culture, as explained by ENISA (2017), embeds awareness training and risk mitigation which in this regard, would be centred around cybersecurity

practices, into everyday work activities, thus establishing a standard for good conduct that will permeate through the organisation.

However, these views are influenced by the relative difficulty in applying and monitoring the various policies, legislation, and regulations for the management of e-waste disposal, given that there are different government departments responsible for different components of these laws, thus adding various complexities to driving WEEE disposal compliance (Ghosh et al., 2016). Avis (2021) contributes to this notion, noting that even in areas where government policies have been adopted, there may be varying challenges like limited power and resources to ensure that organisations meet their regulatory obligations and government institutions driving the necessary enforcement to ensure compliance to these regulations.

5.3.2 Setting organisational policy directives and managing conformance

The formulation and implementation of cybersecurity frameworks, and measures to manage security strategies are not enough to guard against and protect the sensitive and PII stored on various media within organisations (Alqahtani & Braun, 2021). Consideration also needs to be given to the technical knowledge and abilities of the human resources that have a significant influence on the impact of cybersecurity policies and controls (Alqahtani & Braun, 2021).

This can be associated with the approach described by Donaldson et al. (2015, p. 24), as organisations put in place policies that detail specific components within the cybersecurity and e-waste management landscape, and describe the consequences for any violation and non-conformance to these policies.

Kuo et al. (2020) highlight that attention needs to be placed on how the constructs and individual behaviours, as formulated in the deterrence theory, can drive policy compliance in organisations.

Additionally, studies conducted by Tang et al. (2015), consider the effects of organisational culture which is believed to be one of the essential factors contributing to the success or failure of employee compliance to information and cybersecurity policies within organisations. This could be attributed to the belief that employees' behaviour is related to the conformance of set policy frameworks derived from formal directives, but also influenced by visible and observable actions from their leaders (Connolly et al., 2016; Dols & Silvius, 2010).

I. E-waste policy development and implementation

Our study highlights that organisational policies are implemented from a group perspective, and employ a top-down approach in relation to implementation and management practices. The defined policies generally cover the critical elements when looking at cybersecurity, but there is a shared appreciation that some more work and effort is required around e-waste management practices, specifically the general awareness around the disposal of devices when they have reached their EOL with specific focus on devices owned by employees and sometimes utilised for work purposes under the BYOD framework.

Ameen et al. (2021) note that the culture within organisations has an impact on employees' information or cyber-security compliance through the various tiers and levels as they are cascaded through the organisation. This can be influenced

by the culture and behaviour of top-level executives and how they drive and manage their employees to follow prescribed policy practices and conform to set policy frameworks (Connolly et al., 2016).

A point that was further highlighted was that in certain instances, some operational device management functions were passed off to other functional areas and that there is no clear awareness as to the process that is followed around those specific practices. An example of this was the fact that one respondent was responsible for the management of all assets within the organisations, but when they have reached their EOL or are to be disposed of this, would be passed over to another department but was not clear as to the practices specifically at a policy level that occurred there.

This is in contrast to what is recommended by Donaldson et al. (2015, p. 24), who indicate that in most organisational settings, employees will often report into different functional structures or departments, and these functional areas should be carefully organised so that their areas' authority, responsibility, and different levels of expertise are all aligned and synchronised with each other. This will ensure that everyone in the value chain is aware of what is happening, both upstream and downstream of their functions.

II. Policy awareness and training interventions

From our study, we are able to draw out that, in relation to both conformance to regulatory and internal organisational policy, a pivotal area is how these policies are implemented, practised, and complied to. What emerged is that there is a great need for organisations to create awareness with specific focus being placed around data management and DDP thus driving the correct level of compliance

and conformance to implemented policy. However, the awareness drive needs to be supplemented with continual training interventions to reinforce the importance of these practices.

Organisations across the world set aside large amounts of their financial resources to manage their cybersecurity infrastructure, which predominantly looks at technical and non-technical measures (Alqahtani & Braun, 2021). However, a component that is too often neglected but one of the most notable critical elements, with the potential to pose the greatest threat, is the human resource. (Alqahtani & Braun, 2021).

This links to a notable aspect related to awareness denoted by Allam et al. (2014), that most awareness and training efforts within organisations focus on once-off or annual training and awareness interventions, with very limited monitoring post these interventions which have an impact on the behaviour and effective response of individuals to cybersecurity related threats over time.

A view supported by Borthakur and Govind (2017), Gu et al. (2017), and Patil and Ramakrishna (2020), who argue that the complexity of the problem is related to the upsurge of the lack of awareness from individuals with regards to efficient and sustainable e-waste management and DDP.

This can be associated with the construct of Behavioural Intention, as detailed in Figure 7 below, to understand how the training and awareness will assist in driving individuals to perform or behave in an intended way (Kan & Fabrigar, 2017). Coupled to this, we also consider how individuals from the e-waste companies are likely to behave in instances where they are confronted with the acceptance of components from informal trade, specifically focusing on

individuals who do not prescribe to the correct disposal methodologies but are seeking an income, and how this drives the aspect of non-conformance to the processes and associated policy standards, due to these gaps in the regulatory environment.

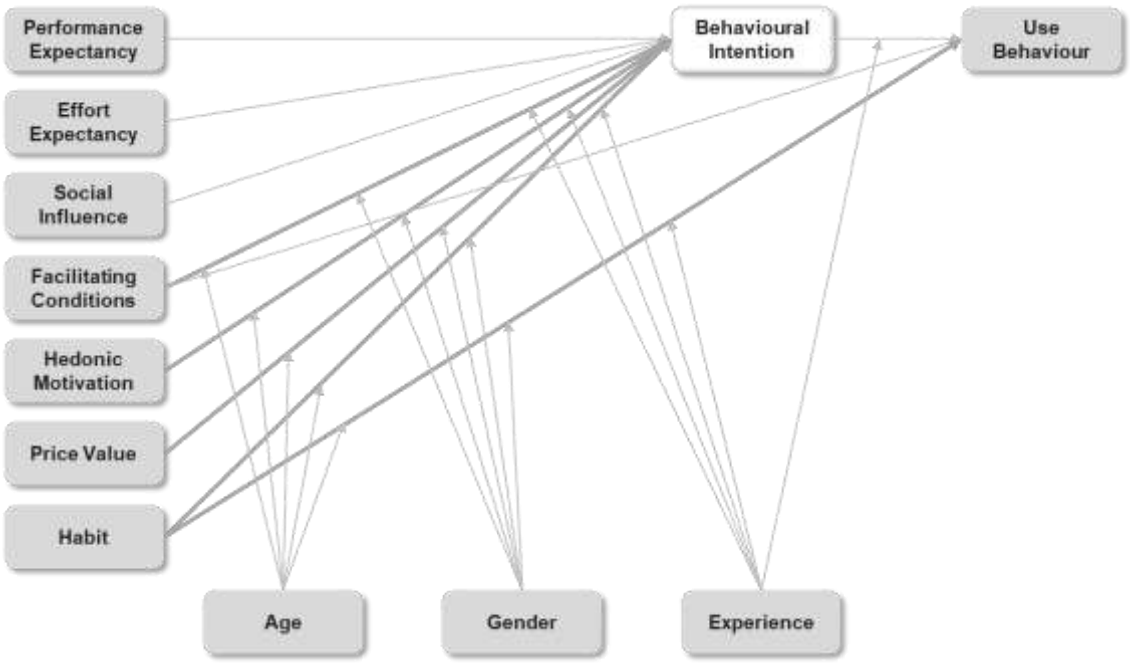


Figure 7: UTAUT2 Model (Alqahtani & Braun, 2021) – Behavioural Intention construct applied to analysis

5.4 Conclusion

In this chapter, we discussed the key findings that emerged from the study and together with various literature reviewed, we unpacked, and in detail, discussed the findings regarding the research objective which sought to assess the vulnerabilities to which organisations are exposed, specifically financial and government institutions, by interrogating the management policies and operations for stored data when disposing of e-waste at the end of asset life cycle and to address the propositions detailed in Chapter 2.

From the discussions, we found that there is a general concern at the rate at which e-waste is generated, and the technological mechanisms available to safely dispose of and discard these devices are significantly outpaced by technological and digital innovation of the devices being manufactured and brought into the market (Schafer, 2014). This has raised certain flags in the industry as most orginasitions are still trying to curb the general cybersecurity threat vectors whilst still trying to understand this new area of data management and device disposal.

Added to this complexity is how orgainsations deal with BYOD and shadow IT with the growing advent of remote working which was exacerbated by the Covid pandemic, which has also exposed a lot of vulnerabilities in both how individuals safeguard their personal technological infrastructure and also how organisations have realised that there is much they still need to focus on when looking at the cybersecurity policies related to this topic.

Organisations need to start taking a more holistic approach to the formulation and implementation of cybersecurity frameworks and facilitate effective measures to manage organisational security strategies (Alqahtani & Braun, 2021). This will facilitate the creation of the right level of awareness and training, which can be cascaded through all the structures within the organisation to protect the sensitive and PII stored on various media within organisations' technological infrastructure (Alqahtani & Braun, 2021).

Coupled to this is the requirement for increased involvement of government and industry role players in creating a synergistic environment, where they are able to formulate robust policy frameworks that can be taken and implemented

throughout the e-waste value chain. Instruments and mechanisms need to be put in place to effectively measure conformance and that those found not complying be held accountable. This will include measures for how government is held accountable for not enforcing and monitoring the policy directives and frameworks that they have put into place.

The following chapter concludes the study and provides recommendations and suggestions for future research.

6 CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This chapter concludes the research, presents recommendations based on the results and makes suggestions for future research.

This study assessed the vulnerabilities to which financial and government institutions are exposed when disposing of e-waste at the end of the asset life cycle. The study further explored how these institutions comply with national legislation, regulations, and standards relating to the management and processing of PII and sensitive organisational data.

From the literature, it emerged that the continued advances in the technology landscape had brought about enhancements, both to organisations and society. The focus is on the utilisation of technologies and the increased importance of data and how it is managed. However, this has also come with unintended challenges, specifically the threats of malicious access to the data generated and utilised on these devices, due to vulnerabilities created within the ecosystem.

The literature further detailed the growing concerns around the effective policy regulations put in place to manage the disposal practices of e-waste and the management of data by various individuals. This is to try and minimise the overall impact it poses to the environment and the entire value chain, at that juncture where electronic devices have reached their EOL and are now being disposed of.

6.2 Understanding the disposal practices organisations put in place to facilitate responsible e-waste management

For organisation to effectively guard and protect themselves against the various cyber and data security related risks, they need to ensure that they have defined and implemented robust organisational policies. These policies need to further extend to and align with their disposal partners, and any parties with whom they are involved through their value chain, therefore ensuring that they all prescribe to effective and responsible e-waste DDP. Coupled to this is the growing requirement to have in place effective data managed frameworks and procedures in place to generally manage PII and any data that is deemed to be of a sensitive nature.

With organisations looking at various mechanisms to manage cost and IT infrastructure, the application of BYOD and services like Shadow IT has meant that organisations relook the various security frameworks and internal technology architecture as they try to enhance and implement policies that the individual or employees will understand and interpret to ensure that they are able to comply to these policies.

It is relatively easy for this to be managed at an internal organisational level, the key challenge organisations face is how this can be extended to their employees on a personal level and secondly, how they manage and engage with their third-party disposal partners.

From our study, we found that when we consider DDP and responsible e-waste and data management at an individual level, the difficulty derived is that if the

right level of awareness is not created, and their employees' behavioural intention does not continue from and link up to the organisational culture. It becomes difficult for employees to prescribe to responsible DDP at a personal level, which could inherently result in PII and sensitive organisational data being compromised when devices are disposed of at EOL. Organisations need to look at training and awareness interventions, and deterrence mechanisms that will bridge this gap and ensure that employees do not necessarily view cybersecurity at work and at home as two separate worlds, but rather as a mutually inclusive environment, specifically when using their own personal devices for the purpose of work.

Another level that is key is the management of third-party suppliers or disposal partners. Organisations should not use the fact that they have contracts in place as an excuse to become complacent. They are required to ensure that they constantly engage, monitor, and measure their third-party suppliers or disposal partners with well-established chain-of-custody measures, and ensure that they are constantly keeping abreast of the various developments related to disposal practices and responsible e-waste and data management. This will ensure that they are able to safeguard their customers' PII that they utilise for various operational purposes, and ensure that their reputation is not tainted due to breaches that could have emanated from vulnerabilities in their supplier's cybersecurity and disposal management processes.

6.3 The impact of cybercrimes on an organisation when proper of disposal methods are not adopted

As the digital landscape continues to grow and evolve due to technological innovation so too will the prominence of data, as its value rises and it becomes an increasingly valuable commodity for various economies and within society through a multitude of technological enablers. However, with this rise in the value of data, so too will there be an increase of threats as criminals seek to exploit any vulnerabilities to use for ill gains and malicious intentions.

The growing rise of e-waste has brought about a new avenue for these criminals to look to, as these avenues have opened new opportunities for devices that have been discarded as WEEE, and they now utilise specific mechanisms of retrieving PII from devices. This in part, has contributed to the fact that relatively few interventions have been put in place to manage data cleansing of devices when disposing of electronic equipment, specifically at an individual consumer level.

From the research study, we found that for organisations, even though a lot of their IT security policies and procedure have been adapted to focus on the prominent rise in cybersecurity threat vectors, some measures have been put in place to manage data and disposal of equipment to minimise the likelihood of any breach. However, it was found that with the rise in organisations adopting policies that allow their employees to work remotely and also the rise in BYOD, it has created difficulties in managing these devices, specifically when they reach a point where they are no longer economically viable for the employee and are then discarded.

This is further fuelled by the fact that many individuals have an over-reliance on the built-in security features of their devices and are not particularly aware of the amount of PII that resides on their devices even after having completed rudimentary wiping or erasing of data on their devices. They are also unaware of how easy it is for cyber hackers to retrieve this PII, with the right tools if, the correct cleansing and disposal methods have not been prescribed to.

From this, we find that there is a need to drive greater awareness with regard to the various cybersecurity threats to which individuals could be exposed. There is also a need to create synergies, with stringent policies and robust interventions that drive how these threats are managed and mitigated at both a professional level, and can be seamlessly applied at a personal level, specifically given that these environments are so closely interlinked.

6.4 The impact national governance policy enforcement has on the level of conformance of organisations

Government plays a critical role in setting the direction in terms of how organisations implement and comply with published policies and standards. Over the years, with the rise of e-waste, both locally and globally, government has started to appreciate the complexity of the various e-waste and data management streams, based on the various facets involved in their management which has opened up and sparked the need to create and develop more focused and specific frameworks that address each of the components on their merits, bringing together these functions and creating an integrated e-waste and data management policy. This is seen in the recent publication of the EPR policy

providing direction into the management of e-waste and the involvement of producers and all individuals and consumers throughout the value stream.

One of the areas that government needs to focus on, is becoming more deliberate in how they enforce these policies and ensure that the defined standards are conformed to. It is imperative that the e-waste and data management sector get to levels where they are as formally regulated as the various other structures in the South African sectoral and organisational landscape. Industry role players and practitioners need to play a more active role in supporting government in providing insights and suggestions to ensure these policies are implementable, sustainable, and that robust measures are put in place and enforced to ensure that all parties are held accountable for the respective roles they play in this ecosystem.

This should be followed by how organisations are able to translate these regulations into organisational level policies that are aligned to their overall strategies. The basis of this is that each and every one, from executive's right down to the lowest level in the organisation understands and buys into the embedded culture and that this drives a set behaviour in relation to compliance. This is dependent on the training and awareness created within organisations, and how this translates into the habitual performance of individuals. This is influenced by both the professional organisational setting and also the personal social setting in relation to how they view e-waste and data management and the associated disposal practices of devices that have reached their EOL and are to be discarded.

These behavioural aspects could set the foundations for organisations meeting their regulatory obligations and set the tone for the establishment of a well-entrenched culture of compliance to overall defined policy frameworks and conformance to set policy standards.

6.5 Recommendations

Through our study, we were able to identify and highlight the various challenges faced by the South African e-waste ecosystem, which is dependent on how it is handled in the coming years and has the potential to have a serious impact, not only on organisations but on society at large. In this section, we look at some recommendations that could be extended to the various facets of the ecosystem in relation to the effective management of data and e-waste disposal practices.

I. The evidence presented suggests that to date, e-waste has not been managed as a separate waste stream, and up until the recent publication of the EPR regulation that no specific focus was placed on e-waste. However government needs to look at putting in place more robust e-waste policies that focus on the entire value chain, with a dedicated focus on how each part of the chain is managed and regulated

II. Government with the involvement from industry needs to work at creating more formalised disposal structures with proper facilities and infrastructure that could effectively support and drive to improve the collection and disposal practices for EOL devices by:

a. Driving more rigorous training and awareness campaigns for everyone involved in the ecosystem to ensure that everyone is informed on what role they play in the disposal cycle
b. Driving the implantation of formalised and regulated structures to manage all the sectors of the e-waste disposal and recycling ecosystem
c. Devising payment methods to facilitated the regulation and formalisation of the sale of these items to ensure that they remove the possibility of exploitation and also create a mechanism for a controlled and structured income stream for the waste pickers

III. Through structured frameworks in their ITAM and ITAD plans, organisations could look at including mechanisms that facilitate the disposal of BYOD that were used by employees, through the internal platforms or infrastructure used to dispose of organisational EOL devices. This will potentially provide an avenue for individuals to use these platforms to dispose of their personal devices in a more secure and controlled manner.

6.6 Suggestions for further research

While the literature points to many studies relating to the gaps in the current policies and how they only focus on the management of general waste and included e-waste into this broader categorisation, no specific focus has been placed on how it should be managed in the industry as this topic has not been studied in much detail. It is only now that e-waste is receiving the required attention as its prominence in both global and local arenas continues to grow,

providing a new perspective to the various vulnerabilities that organisations and individuals can be exposed to when electronic devices are being disposed of. In this section, we expand on the various issues that emerged from the study which serve as potential contributions for further research.

I. Understanding whether technology acceptance models have an impact on and can influence training and awareness around e-waste and data management in organisations, and how this will drive improved conformance to effective DDP and the management of data for devices that have reached their EOL.

II. Assessing the data management and DDP in various sectors and performing a comparative analysis on how these compare across these sectors. This is to establish performance variances across industries and establish whether generic or sector specific policies are required to manage the South Africa e-waste ecosystem.

III. Assessing how the effects of the Covid 19 pandemic have impacted organisations in relation to unauthorised access to PII, due to theft as a result of the rise in unemployment.

IV. Using the UTAUT2 framework to analyse whether South African organisations have experienced an increase or decrease in relation to cybersecurity policy compliance due to work from home policies implemented.

V. Assess whether the lack of a specifically focused and formalised e-waste policy is impeding the creation of a well-regulated e-waste industry or sector.

REFERENCES

Adams, R., Adeleke, F., Anderson, D., Bawa, A., Branson, N., Christoffels, A., Vries, J. d., Etheredge, H., Flack-Davison, E., Gaffley, M., Marks, M., Mdhluli, M., Mahomed, S., Molefe, M., Muthivhi, T., Ncube, C., Olckers, A., Papathanasopoulos, M., Pillay, J., Schonwetter, T., Singh, J., Swanepoel, C., & Ramsay, M. (2021). POPIA Code of Conduct for Research. *Discussions on POPIA: POPIA Code of Conduct for Research, 117*(5/6), 1-12. https://doi.org/https://doi.org/10.17159/sajs.2021/10933

Alghazo, J., Ouda, O. K. M., & Hassan, A. E. (2018). E-waste environmental and information security threat: GCC countries vulnerabilities. *Euro-Mediterranean Journal for Environmental Integration, 3*(1). https://doi.org/10.1007/s41207-018-0050-4

Allam, S., Flowerday, S. V., & Flowerday, E. (2014, May). Smartphone information security awareness_A victim of operational pressures. *Computers & Security 42*, 56-65. https://doi.org/DOI:10.1016/j.cose.2014.01.005

Alqahtani, M., & Braun, R. (2021). Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review. *Journal of Information Assurance & Cybersecurity, 2021*, 1-15. https://doi.org/10.5171/2021.666987

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*. https://doi.org/10.1016/j.chb.2020.106531

Anney, V. N. (2014). Ensuring the Quality of the Findings of Qualitative Research. *Journal of Emerging Trends in Educational Research and Policy Studies (JETERAPS), 5*(2), 272-281. http://196.44.162.10:8080/xmlui/bitstream/handle/123456789/256/Ensuring%20the%20Quality%20of%20the%20Findings%20of%20Qualitative%20Research%20NEW.pdf?sequence=1&isAllowed=y

Avis, W. (2021). *Drivers, barriers and opportunities e-waste management in Africa* (Helpdesk Report, Issue.

https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/17152/1071_E-Waste_Management.pdf?sequence=1

Balushi, K. A. (2018, April). The Use of Online Semi-Structured Interviews in Interpretive Research. *International Journal of Science and Research, 7*(4), 726-732. https://doi.org/10.21275/ART20181393

Bhardwaj, P. (2019, 2019 December 20). Types of Sampling in Research. *Journal of the Practice of Cardiovascular Sciences, 5*, 157-163. https://doi.org/10.4103/jpcs.jpcs_62_19

Bob, U., Padayachee, A., Gordon, M., & Moutlana, I. (2017). Enhancing Innovation and Technological Capabilities in the Management of E-Waste: Case Study of South African Government Sector. *Science, Technology and Society, 22*(2), 332-349. https://doi.org/10.1177/0971721817702293

Borthakur, A. (2020). Policy approaches on E-waste in the emerging economies: A review of the existing governance with special reference to India and South Africa. *Journal of Cleaner Production, 252*. https://doi.org/10.1016/j.jclepro.2019.119885

Borthakur, A., & Govind, M. (2017). Emerging trends in consumers' E-waste disposal behaviour and awareness_A worldwide overviewwith special focus on India. *Resources, Conservation and Recycling, 117*, 102-113. https://doi.org/doi:10.1016/j.resconrec.2016.1

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

BritishBroadcastingCorporation. (2021, June 09). *G7: 'Mount Recyclemore' of leaders made from electronic waste in Cornwall*. BBC News Retrieved 2021 June 15 from https://www.bbc.com/news/uk-england-cornwall-57406136

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing, 25*(8), 652-661. https://doi.org/10.1177/1744987120927206

Chang, A. (2012). View of UTAUT and UTAUT 2: A Review and Agenda for Future Research. *The Winners, 13*(2), 106-114. https://doi.org/https://doi.org/10.21512/tw.v13i2.656 (28 September 2012)

Chigada, J., & Daniels, N. (2021). Exploring information systems security implications posed by BYOD for a financial services firm. *Business Information Review, 38*(3), 115-126. https://doi.org/DOI:10.1177/02663821211036400

Cho, V., & Ip, W. H. (2017, November 15). A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems, 12*(6), 659-673. https://doi.org/https://doi.org/10.1080/17517575.2017.1404132

Connolly, L., Lang, M., Gathegi, J., & Tygar, J. D. (2016). The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study. *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 33-44. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwia7bXNoe31AhWKi1wKHWmHAyAQFnoECAMQAQ&url=https%3A%2F%2Fwww.cscan.org%2Fopenaccess%2F%3Fid%3D292&usg=AOvVaw3OXRmvvfL91q_ztaZD8W4_

Creswell, J. W., & Creswell, J. D. (2018). *Research_Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5 ed.). SAGE Publications Ltd.

CXOtodayNewsDesk. (2021, June 15). *G7 Summit Turns Spotlight on Crypto-Led Ransomware Attack*. CXOtoday News Desk. Retrieved 2021 June 15 from https://www.cxotoday.com/news-analysis/g7-summit-turns-spotlight-on-cybersecurity-ransomware/

de Froberville, P. (2019). *Electronic waste –The toxic legacy of our digital age*. Golegal. Retrieved 2021 May 13 from https://www.golegal.co.za/e-waste-treatment-facilities/#:~:text=As%20stated%20above%2C%20e%2Dwaste,rapidly%20growing%20global%20waste%20problem.&text=According%20to%20the%20e%2DWaste,12%25%20of%20that%20is%20recycled.

Debnath, B. D., Das, S., & Das, A. (2019, September, 4). Study Exploring Security Threats in Waste Phones. https://ssrn.com/abstract=3443923

DLAPiper. (2021, 2021 December 20). *Data Protection Laws of the World*. DLA Piper. Retrieved July 6 from https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=ZA

Dols, T., & Silvius, A. J. G. (2010). Exploring the Influence of National Cultures on Non-Compliance Behavior. *Communications of the IIMA, 10*(3). https://scholarworks.lib.csusb.edu/ciima/vol10/iss3/2?utm_source=scholarworks.lib.csusb.edu%2Fciima%2Fvol10%2Fiss3%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (1 ed.). Apress. https://doi.org/10.1007/978-1-4302-6083-7

Downer, K., & Bhattacharya, M. (2015). *BYOD Security: A New Business Challenge* 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity),

Dudovskiy, J. (n.d). *Purposive sampling*. Business Research Methodology. Retrieved 2021 June 28 from https://research-methodology.net/sampling-in-primary-data-collection/purposive-sampling/

EACO. (2013). *EACO Model Framework for E-waste Management*. http://www.eaco.int/admin/docs/reports/Policy_Model_Framework_June_2013.pdf

ENISA. (2017, November). Cyber Security Culture in organisations *European Union Agency For Network and Information Security*. https://doi.org/10.2824/10543

Environment, D. F. F. (2015). Minister Molewa leads National Consultative Conference on Electronic and Electrical Waste (E-Waste) Management in South Africa. National Consultative Conference on Electronic and Electrical Waste (E-Waste) Management in South Africa, Birchwood Hotel and Conference Centre in Gauteng.

ERI-Direct. (2018). *Formulating An Asset Disposition (ITAD) Plan In The Financial Services Industry*. ERI-Direct. Retrieved 2021 May 24 from https://eridirect.com/blog/2018/02/formulating-an-asset-disposition-itad-plan-in-the-financial-services-industry/

Escobar-Rodríguez, T., & Carvajal-Trujillo, E. (2014, 2014 August). Online purchasing tickets for low cost carriers: An application of the UTAUT model. *Tourism Management, 43*, 70-88. https://doi.org/https://doi.org/10.1016/j.tourman.2014.01.017

Eslahi, M., Naseri, M. V., Hashim, H., Tahir, N. M., Hisham, E., & Saad, M. (2014, April 7 - 8). BYOD Current State and Security Challenges. *IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. https://doi.org/https://doi.org/10.1109/ISCAIE.2014.7010235

Finlay, A. (2007, November 30). E-waste Challenges In Developing Countries: SA Case Study. [Discussion paper]. https://www.apc.org/en/pubs/issue/e-waste-challenges-developing-countries-south-afri

Finlay, A., & Liechti, D. (2008). e-Waste Assessment South Africa. *e-Waste Association of South Africa (eWASA)*.

Forgor, L., Brown-Acquaye, W., Arthur, J. K., & Owoo, S. (2019). Security of Data on E-waste equipment to Africa_The Case of Ghana. *2019 International Conference on Communications, Signal Processing and Networks (ICCSPN)*, pp. 1-5. https://doi.org/doi: 10.1109/ICCSPN46366.2019.9150166

Forti, V., Baldé, C. P., Kuehr, R., & Be, G. (2020). *Global E-waste Monitor 2020*.

Friedmana, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management, 7*, 159–180.

Ghosh, S. K., Debnath, B., Baidya, R., De, D., Li, J., Ghosh, S. K., Zheng, L., Awasthi, A. K., Liubarskaia, M. A., Ogola, J. S., & Tavares, A. N. (2016, August 22). Waste electrical and electronic equipment management and Basel Convention compliance in Brazil, Russia, India, China and South Africa (BRICS) nations. *Waste Manag Res, 34*(8), 693-707. https://doi.org/10.1177/0734242X16652956

Gu, F., Ma, B., Guo, J., Summers, P. A., & Hall, P. (2017, Oct). Internet of things and Big Data as potential solutions to the problems in waste electrical and electronic equipment management: An exploratory study. *Waste Manag, 68*, 434-448. https://doi.org/10.1016/j.wasman.2017.07.037

Haag, S., & Eckhardt, A. (2017). Shadow IT. *Business & Information Systems Engineering, 59*(6), 469-473. https://doi.org/10.1007/s12599-017-0497-x

Heeks, R., Subramanian, L., & Jones, C. (2014). Understanding e-Waste Management in Developing Countries: Strategies, Determinants, and Policy Implications in the Indian ICT Sector. *Information Technology for Development, 21*(4), 653-667. https://doi.org/10.1080/02681102.2014.886547

Huffington-Post. (2017). *Why E-waste Should be at the Forefront of a Company's Cybersecurity Plan*. ERI Direct. Retrieved 2021 May 14 from https://eridirect.com/blog/2017/09/why-e-waste-should-be-at-the-forefront-of-a-companys-cybersecurity-plan/

Ichikowitz, R., & Hattingh, T. (2020). Consumer E-Waste Recycling in South Africa. *South African Journal of Industrial Engineering, 31*(3). https://doi.org/10.7166/31-3-2416

Ikhlayel, M. (2018). An integrated approach to establish e-waste management systems for developing countries. *Journal of Cleaner Production, 170*, 119-130. https://doi.org/10.1016/j.jclepro.2017.09.137

IOL, S. R. (2019). *Massive penalties for data breaches*. IOL. Retrieved 2021 July 3 from https://www.iol.co.za/business-report/companies/massive-penalties-for-data-breaches-31822314

Jones, A. (2009, November). Recycling more than your IT equipment. *Network Security, 2009*(11), 8-9. https://doi.org/https://doi.org/10.1016/S1353-4858(09)70121-7

Kan, M. P. H., & Fabrigar, L. R. (2017). Theory of Planned Behavior. In *Encyclopedia of Personality and Individual Differences* (pp. 1-8). https://doi.org/10.1007/978-3-319-28099-8_1191-1

Kumar, A., Holuszko, M., & Espinosa, D. C. R. (2017). E-waste: An overview on generation, collection, legislation and recycling practices. *Resources, Conservation and Recycling, 122*, 32-42. https://doi.org/10.1016/j.resconrec.2017.01.018

Kuo, K.-M., Talley, P. C., & Huang, C.-H. (2020, November). A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. *Computers & Security, 96*. https://doi.org/https://doi.org/10.1016/j.cose.2020.101928

Lawhon, M. (2013). Dumping Ground or Country-in-Transition? Discourses of E-Waste in South Africa. *Environment and Planning C: Government and Policy, 31*(4), 700-715. https://doi.org/10.1068/c1254

MacFeely, S., Me, A., Fu, H., & Schweinfest, S. (2020). *We urgently need a Global Data Convention. Here's why*. World Economic Forum. Retrieved 2021 June 27 from https://www.weforum.org/agenda/2020/11/global-data-convention/

Maphosa, V., Maphosa, M., & Tan, A. W. K. (2020). E-waste management in Sub-Saharan Africa: A systematic literature review. *Cogent Business & Management, 7*(1). https://doi.org/10.1080/23311975.2020.1814503

Marks, K. (2011, October 10). *ITAD Chain of Custody*. The ITAM Review. Retrieved January 28 from https://www.itassetmanagement.net/2011/10/10/itad-chain-custody/

Mihai, A. (2021). *Hacking E-waste is the "greatest little secret" of cyber-security, and it's worth paying attention*. Heidelberg Laureate Forum Foundation. Retrieved 2021 May 13 from https://www.newsroom.hlf-foundation.org/blog/article.html?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=285&cHash=d96c53bc9cc7dab1e56315d944f49c9d

Morrow, B. (2012). BYOD security challengescontrol and protect your most sensitive data. *Network Security*, 5-8. https://doi.org/https://doi.org/10.1016/S1353-4858(12)70111-3

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis. *International Journal of Qualitative Methods, 16*(1). https://doi.org/10.1177/1609406917733847

Pathak, V. C. (2017). Phenomenological Research A Study of Lived Experiences. *3* (1). http://ijariie.com/AdminUploadPdf/Phenomenological_Research__A_Study_of_Lived_Experiences_ijariie3960.pdf

Patil, R. A., & Ramakrishna, S. (2020, March 20). A comprehensive analysis of e-waste legislation worldwide. *Environmental Science and Pollution Research*. https://doi.org/https://doi.org/10.1007/s11356-020-07992-1

Perkins, D. N., Brune Drisse, M. N., Nxele, T., & Sly, P. D. (2014, Jul-Aug). E-waste: a global hazard. *Ann Glob Health, 80*(4), 286-295. https://doi.org/10.1016/j.aogh.2014.10.001

Plambeck, E., & Wang, Q. (2009). Effects of E-Waste Regulation on New Product Introduction. *Management Science, 55*(3), 333-347. https://doi.org/10.1287/mnsc.1080.0970

Sabillon, R., Cavaller, V., & Cano, J. (2016, May). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering, 5*(5), 67-81. http://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf

Sari, D. P., Masruroh, N. A., & Asih, A. M. S. (2021, March 4). Consumer Intention to Participate in E-Waste Collection Programs: A Study of Smartphone Waste in Indonesia. *Sustainability, 13*(5). https://doi.org/10.3390/su13052759

SAWIC, S. (n.d, 2016 December 4). *Waste Policy and Regulations*. Retrieved June 11 from http://sawic.environment.gov.za/?menu=13

Schafer, B. (2014). D-waste: Data disposal as challenge for waste management in the Internet of Things. *International Review of Information Ethics, 22*

Schepers, M., & Novazi, Z. (2020). *South Africa: The Destruction Or Deletion Of Personal Information In The POPIA Era*. Andersen. Retrieved January 15 from https://www.mondaq.com/southafrica/privacy-protection/990256/the-destruction-or-deletion-of-personal-information-in-the-popia-era

Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of Shadow IT on Innovation in Organizations. *Complex Systems Informatics and Modeling Quarterly*(8), 68-80. https://doi.org/10.7250/csimq.2016-8.06

Sinkovics, R. R., Penz, E., & Ghauri, P. N. (2009). Enhancing the Trustworthiness of Qualitative Research in International Business. *Management International Review, 48*(6), 689-714. https://doi.org/10.1007/s11575-008-0103-z

Sovacool, B. K. (2019). Toxic transitions in the lifecycle externalities of a digital society: The complex afterlives of electronic waste in Ghana. *Resources Policy, 64*. https://doi.org/10.1016/j.resourpol.2019.101459

Tang, M., Li, M. g., & Zhang, T. (2015, January 15). The impacts of organizational culture on information security culture: a case study. *Information Technology Management*. https://doi.org/DOI 10.1007/s10799-015-0252-2

Tanskanen, P. (2013). Management and recycling of electronic waste. *Acta Materialia, 61*(3), 1001-1011. https://doi.org/10.1016/j.actamat.2012.11.005

Thing, V. L. L., & Tan, D. J. J. (2012). Symbian Smartphone Forensics and Security: Recovery of Privacy-Protected Deleted Data. *Information and Communications Security, 7618*, 240–251. https://doi.org/https://doi.org/10.1007/978-3-642-34129-8_21

Trueman, C. (2019). *Why data centres are the new frontier in the fight against climate change*. Computerworld. Retrieved 2021 September 13 from https://www.computerworld.com/article/3431148/why-data-centres-are-the-new-frontier-in-the-fight-against-climate-change.html

Upton, S. (2021, 10 June 2021). *Scaling The Mountain Of Electronic Waste*. TwoSides. Retrieved June 15 from https://www.twosides.info/UK/mount-recyclemore-electronic-waste/

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: A Case Study From a South African Organisation. *The Electronic Journal Information Systems Evaluation, 22*(1), 1-14. https://academic-publishing.org/index.php/ejise/article/view/124/87

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY. *Forthcoming in Journal of the Association for Information Systems,, 17*(5), 328–376. https://doi.org/http://dx.doi.org/10.17705/1jais.00428

Warner, J., Abugri, G. S., Warren, P., Marks, K., Hutchison, K., & Goldsmith, P. (2012, November). Feature: exploring the links between cybercrime and e-waste. *ADISA Magazine*, (2), 5-15. https://adisa.global/wp-content/uploads/magazines/ADISA%20Magazine_Issue%2002.pdf

Washtell, F. (2022). *Cyber hacking soars as staff working from home can be vulnerable to data breaches, research suggests*. The Daily Mail. Retrieved February 2 from https://www.dailymail.co.uk/news/article-10458465/Cyber-hacking-soars-staff-working-home-vulnerable-data-breaches-research-suggests.html

Wattles, J., & Larson, S. (2017). *How the Equifax data breach happened: What we know now*. CNNMoney. Retrieved July 3 from https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

Whitty, M. T. (2018). 419 – It's just a Game: Pathways to CyberFraud Criminality emanating from West Africa. *International Journal of Cyber Criminology 12*(1), 97–114. https://doi.org/10.5281/zenodo.1467848

William, C. A. (2015). Conducting Semi-Structured Interviews. In *Handbook of Practical Program Evaluation,* (Fourth Edition ed., pp. 492-505). Jossey-BassEditors: J. Wholey, H.Hatry, K. Newcomer. https://doi.org/doi:10.1002/9781119171386.ch19

WorldEconomicForum. (2020). *WEF: New Paradigm for Business of Data_Report 2020*. https://www.weforum.org/agenda/2020/07/new-paradigm-business-data-digital-economy-benefits-privacy-digitalization

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2009). *Business Research Methods* (8 ed.). South-Western Cengage Learning.

APPENDIX A: Information sheet

Good day Sir / Madam,

My name is Dimitri Khumalo and I am a Masters of Management student in the field of Digital Business at the University of the Witwatersrand, Johannesburg. As part of my studies, I have to undertake a research project, and I am investigating cybersecurity vulnerabilities in the disposal of e-waste in South African Public & Private Institutions under the supervision of Dr Kiru Pilly. The aim of this research project is to assess the vulnerabilities organisations are exposed to, by interrogating the management policies and operations for stored data when disposing of e-waste at the end of asset life cycle and explore how these institutions comply with the national legislations, regulations, and standards relating the management of personal and sensitive data.

As part of this project, I would like to invite you to take part in an interview. This activity will involve a face-to-face interview session with a set of closed and open-ended questions in line with the defined topic and will take around 60 minutes. With your permission, I would also like to audio record the interview using a digital device. This recording will be stored in digitally encrypted folder on a password protected computer and only the researcher will have access to this recording. It will be deleted after 5 years.

If you have any questions during or afterwards about this research, feel free to contact me on the details listed below. This study will be written up as a research report which will be available online through the university library website. If you wish to receive a summary of this report, I will be happy to send it to you (optional). The data collected from this research project will be stored in digitally encrypted folder on a password protected computer and will be kept for 5 years If you have any concerns or complaints regarding the ethical procedures of this study, you are welcome to contact the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za

Yours sincerely,

Dimitri Khumalo

Researcher:

Dimitri Khumalo, Dimitri.Khumalo1@students.wits.ac.za, 079 885 3837

Supervisor:

Dr Kiru Pillay, kiru2010@gmail.com, 082 602 7261

APPENDIX B: Agreement form

Assessing cybersecurity vulnerabilities in the disposal of e-waste in South African Public & Private Institutions

Dimitri Khumalo

I, ……., agree to participate in this research project. The research has been explained to me and I understand what my participation will involve. I agree to the following:

(Please circle the relevant options below).

I agree that my participation will remain anonymous	YES	NO
I agree that the researcher may use anonymous quotes in his / research report	YES	NO
I agree that the interview may be audio recorded, and that I may opt out or stop the session at any point where I do not feel comfortable	YES	NO

(Signed consent will be obtained from the respondent prior to the commencement of the interview)

APPENDIX C: Interview guide

Introduction:

Good Day (Name of Participant) as noted in my earlier request, my name is Dimitri Khumalo and I am a Masters of Management student in the field of Digital Business at the University of the Witwatersrand, Johannesburg.

As part of my studies, I have undertaken to research, and investigate the cybersecurity vulnerabilities in the disposal of e-waste in South African Public & Private Institutions.

As part of this interview, I would like to discuss the following topics:

- Data vulnerabilities and threats (during asset disposal) within the organisation;
- The application of Regulatory policies, directives and frameworks for e-waste and the management of data disposal within organisations; and
- The level of compliance, adherence and monitoring of defined regulatory policies in the organisation.
- *NB: Please note that you are welcome and free to refrain from answering or stop the interview at any stage you do not feel comfortable or are uneasy with the line of questioning*

With these topics in mind the outline of the interview will be structured as follows:

- Opening and introductory questions (general question(s) to set the respondents at ease);
- Middle section of the questionnaire will focus more on in-depth questions based on the defined topics to ascertaining responses in relation to the research; and
- Lastly establish if there are any further details the participant may wish to share that may add value to the research, wrap up and close out the session

Opening / Introductory Question
Q1: Could we start by you telling me a little about your role within your organisations
Follow on / Clarifying question may be asked depending on the answer provided
Comment:
Middle section (Topic Questions)
I would now like to start with some of the topic questions highlighted

Q2: Can you tell me how data (both personal and sensitive) and e-waste are managed through their respective life cycles (specifically at the disposal phase of devices) within your organisation?
Comment:
Q2.1: Have these (data and asset disposal management) been formulated as one policy/plan or two separate policies/plans?
Comments:
Q2.2: How do these policies/plans cater for and make provisions for the management of Shadow IT application and “Bring Your Own Devices” usage, in relation to the disposal practices, within the organisation?
Comments:
Q3: Based on the defined data and e-waste management plans what are some of the key vulnerabilities/threats your organisation has been exposed too?
Comments:
Q3.1: In your opinion, what are the most worrisome elements of these are vulnerabilities/threats?
Comments:
Q4: How much engagement/interaction does your organisation have with your third-party e-waste disposal service providers regarding their e-waste practice in line with your ICT device and data disposal policies?
Comments:
Q4.1: How regularly are they audited to ensure compliance to your organisations ICT device and data disposal requirements?
Comments:
Q5: How much impact or influence has national governance policies had on how your organisations manages e-wastes, specifically the cleansing of data on electronic devices before disposing of them when they have reached their EOL?
Comments:
Q5.1: Do you believe that more can be done in terms of government policies in relation to disposal practices to facilitate responsible e-waste management for

the different categories of Information and Communication Technologies (ICT) devices
Comments:
Q5.2: In your opinion, is enough being done to ensure compliance to these policies and are Government agencies doing enough to enforce the right level of adherence to these policies?
Comments:
Q5.3: Do you have organisational (internal and external) audits conducted in relation to the compliance and adherence to the defined e-waste and data management for the disposal of Information and Communication Technologies (ICT) devices?
Comments:
Q5.4: How frequently are they conducted?
Comments:
Q5.5: How are the findings from these audits managed and resolved or mitigated to ensure no future reoccurrences?
Comments:
Wrap up and close out
Q6: Is there anything else or any additional you may wish to highlight or add that could contribute to the discussion would like to add?
Comments:
Thank the participant for his/her participation and inputs provided during the interview and close the session.

APPENDIX D1: Research code and transcript association

	Respondent 4 Gr=42	Respondent 5 Gr=132	Respondent 6 Gr=82	Respondent 1 Gr=68	Respondent 3 Gr=48	Respondent 8 Gr=90	Respondent 9 Gr=55	Respondent 12 Gr=95	Respondent 11 Gr=72	Respondent 10 Gr=78	Respondent 7 Gr=43	Respondent 2 Gr=10
○ 3rd Party Engagement Gr=14	1	1	3	1	2	1	1	1	1	1	1	1
○ Audits Gr=12	1	1	1	1	0	1	1	2	1	2	1	1
○ Compliance Gr=13	2	2	2	0	0	1	2	1	1	0	2	2
○ Conformance Management Gr=4	0	1	2	0	0	1	0	0	0	0	0	1
○ Data Breaches Gr=25	1	5	1	2	2	2	2	2	2	4	2	2
○ Data Classification Gr=9	1	1	1	0	2	0	1	1	1	0	1	1
○ Data Management Gr=25	3	0	6	0	2	4	2	3	3	2	0	2
○ Device treatment /management Gr=26	2	2	3	2	4	3	1	1	1	6	1	2
○ e-Waste Defined Gr=14	4	1	1	0	2	1	1	1	1	1	1	1
○ Gov Influence on Policy Gr=9	1	1	2	0	0	1	1	0	1	1	1	1
○ Govenmental Involvement/Influence Gr=11	0	0	1	1	1	1	0	1	2	2	2	2
○ Policy Formulation Gr=2	0	0	0	0	0	0	0	0	1	1	0	0
○ Policy/Frameworks Gr=20	2	2	2	1	0	3	2	5	1	1	1	1
○ Shadow IT/BYOD Gr=12	1	2	1	1	1	1	1	1	0	1	2	2
○ Training and awarness creation Gr=8	0	1	1	0	1	1	2	0	1	1	0	1
○ waste management approach Gr=9	1	1	2	0	0	0	1	1	0	3	0	0

APPENDIX D2: Research analysis data association

TITLE						
Assessing cybersecurity vulnerabilities in the disposal of e-waste in South African public & private institutions						
Research question	**Research Propositions**	**Research Sub-Aims**	**Research Instrument questions to adress linked sections**	**Associated Code**	**Emerging Themes**	**People/Participants providing data**
1. Assess how data (both personal and sensitive) is managed within private sector organisations and public sector institutions when disposing of electronic ICT equipment, when these devices have reached their EOL.	1. The researcher through the study seeks to assess the vulnerabilities in the e-waste management with specific focus on how data is managed when disposing of electronic devices utilised in public and private institutions, when they have they have reached their EOL as classified by defined organisational policies.	1.1 Explore the disposal practices public and private sector organisations have put in place to facilitate responsible e-waste management for the different categories of Information and Communication Technologies (ICT) devices	Q 2. Are there currently e-waste policies or e-waste management plans that have been implemented in your organisation? Q 2.1 Can you explain how these policies/plans have been formulated (in other words can you please define how these policy/plan work) within your organisation? Q 2.2 Do these policies/plans cater for, or make provision for the management of data, specifically in relation to the disposal practices of devices that have reached their EOL, within your organisation? Q 2.3 Has the data on these devices been classified (classified/categorised according to sensitivity and business impact to establish levels of risk if exposed)? Q. 2.4 Do these policies/plans cater for and/or make provisions for the management of Shadow IT applications and "Bring Your own devices" with specific focus on the disposal practices of devices that have reached their EOL, within the organisation? Q 4. How much engagement/interaction does your organisation have with your third-party e-waste disposal service providers (how frequently do you engage with the organisations that provide a service too you) regarding e-waste practices in line with ICT devices that have reached EOL and data disposal policies?	1. 3rd Party Engagement 2. Data Classification 3. Data Management 4. Device treatment /management 5. e-Waste Defined 6. Policy Formulation 7. Shadow IT/BYOD 8. Training and awarness creation 9. Waste management approach	1. E-waste policies, directives and frameworks formulation 2. BYOD and Shadow IT management 3. Third party engagement practices	1. Executives (CIO/CDO) responsible for ICT and cyber security in the financial services sector; 2. Directors, Deputy Directors, Senior Managers, or Heads of Departments responsible for Cybersecurity and Infrastructure Management and Security within the in the public/government sector; 3. Senior managers from e-waste recycling companies situated in the Gauteng province in South Africa to participate in this study
		1.2 Investigate the impact of cybercrimes on an organisation when proper methods of disposal are not adapted either by the public and private sector organisations or by the third-party recycling institutions.	Q 3. Based on the policies/plans in place within your organisation, are there any possibilities of data breaches that may emanate from equipment that have reached their EOL? Q 3.1 To your knowledge, have any serious breaches ever occurred in your organisation or any of the 3rd party suppliers that handle the disposal of your EOL devices?	1. Data Breaches 2. Device treatment /management 3. Training and awarness creation	1. Data management and breaches	1. Executives (CIO/CDO) responsible for ICT and cyber security in the financial services sector; 2. Directors, Deputy Directors, Senior Managers, or Heads of Departments responsible for Cybersecurity and Infrastructure Management and Security within the in the public/government sector; 3. Senior managers from e-waste recycling companies situated in the Gauteng province in South Africa to participate in this study
	2. The researcher seeks to assess how better enforcement of regulatory policy has the potential to improve the compliance and responsible behaviour of organisation in relation to the proper management of data during the disposal of e-waste equipment at the EOL	1.3 Explore the impact the enforcement of national governance policies has on the level of conformance of public and private sector organisations to policies governing the cleansing of data on electronic devices before disposing of them when they have reached their EOL.	Q 2.5 How much impact/influence does national government policies have on how your organisation manages e-waste, specifically in relation to the cleansing of data on electronic devices before disposing of them when they have reached their EOL? Q 5 In your opinion, are Government agencies doing enough to ensure the compliance and adherence to the defined e-waste policies? Q5.1 Do you believe that Government agencies are doing enough to ensure that data (both personal and sensitive) is adequately managed and protected (in other words ensuring the compliance and adherence to requirements to the defined e-waste and data management policies) at the disposal phase of devices at their EOL? Q 5.2 What measures (that you are aware of) have been put in place, by these agencies, to ensure the required levels of conformance to defined and implemented policies? Q5.3 Do you have organisational audits (for both internal and 3rd party service providers) that are conducted in relation to the compliance and adherence to the defined e-waste and data management policies when disposing of ICT devices when they have reached their EOL? Q5.4 How frequently are these audits conducted? Q5.5 How are the findings from these audits managed and remediated to ensure mitigation of these incidents (adverse audit findings) to reduce future reoccurrences?	1. Audits 2. Gov Influence on Policy 3. Govenmental Involvement/Influence 4. Policy Formulation 5. Policy/Frameworks 6. Training and awarness creation	1. Government impact on E-waste regulatory policies, directives and frameworks management 2. Governments influence on policy compliance management 3. Policy Awareness and training	1. Executives (CIO/CDO) responsible for ICT and cyber security in the financial services sector; 2. Directors, Deputy Directors, Senior Managers, or Heads of Departments responsible for Cybersecurity and Infrastructure Management and Security within the in the public/government sector; 3. Senior managers from e-waste recycling companies situated in the Gauteng province in South Africa to participate in this study

APPENDIX E: Ethical Clearance Certificate

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/DB2363715/848
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

This certificate is only valid if accompanied by formal permission from the relevant stakeholder(s).

Project title	Assessing cybersecurity vulnerabilities in the disposal of e-waste in South African public & private Institutions
Investigator / Researcher	Mr Dimitri Khumalo
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	2021-08-18
Expiry date	Date of submission of the project 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.

Signature

23/08/2021.
Date: