

Cyber-attack avoidance behaviour in District Health
Information System (DHIS): A case of Tshwane district
healthcare centres

by

THETSHELESANI ANGEL NETSHISHIVHE

submitted in accordance with the requirements for

the degree of

MASTER OF SCIENCE

In the subject

COMPUTING

at the

University of South Africa

Supervisor: Prof Chimbo Bester

Co-Supervisor: Dr. Motsi Lovemore

March 2023

DECLARATION

Name: THETSHELESANI ANGEL NETSHISHIVHE

Student number: 54901995

Degree: MASTER OF SCIENCE IN COMPUTING

TITLE : CYBER-ATTACK AVOIDANCE BEHAVIOUR IN DISTRICT HEALTH
INFORMATION SYSTEM (DHIS): A CASE OF TSHWANE DISTRICT
HEALTHCARE CENTRES

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

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

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



SIGNATURE

07 March 2023

DATE

ACKNOWLEDGEMENTS

Without God, I am nothing, therefore, first of all, I thank God for granting me the wisdom, ability and strength to pursue this study until I successfully completed it. I would like to take this opportunity to express my sincere and deepest gratitude to my supervisors, Professor Bester Chimbo, and Dr Lovemore Motsi, for their invaluable supervision, support, guidance and patience during the course of my Masters degree. I really appreciate their insightful comments, suggestions, advice, wisdom and quick feedback whenever I required reviews. I would also like to apologise for putting them under a lot of strain. This endeavor would not have been possible without them, therefore, I really appreciate their guidance. Words cannot express my gratitude to Dr Tawanda Blessing Chiyangwa for his treasured support, which was essential in shaping my statistical analysis. I would also like to express my most profound gratitude to Professor Alexender Trish for editing and polishing my dissertation, I am extremely grateful for her support, wisdom and input. I am also thankful to the late Ms Suwisa Muchengetwa for her support and guidance during the compiling of the study questionnaire.

To the Gauteng Province department of health, Tshwane regional research ethics committee and Tshwane district healthcare facilities managers, thank you for permitting me to collect data at your facilities. A special thank you to all the participants who took time out of their busy schedules and completed the questionnaire; without you, I would not have the content of this Masters study. I would be remiss not to mention my lovely husband, Muelekanyi Ravhura, for his unwavering love, emotional support, and kind words when I almost gave up. I would like to thank my Mother, sisters, family at large, friends, and daughter Ronewa for keeping my spirit going. Lastly, but yet importantly, I would like to thank myself for all the hard work, dedication, believing in myself, and continuing to put effort into this research until the finish line.

ABSTRACT

Implementing effective cyber-security controls in e-health systems in South Africa, especially those used in hospitals, will help prevent cyber-attacks and protect sensitive data. This study aimed to determine the effective ways of encouraging compliance with the District Health Information System (DHIS) cyber-security controls. In order to accomplish this aim, the researcher investigated how healthcare support staff from the Tshwane District Healthcare Centres who interact directly with the DHIS perceive cyber-attack threats. The Technology Acceptance Model, Technology, Organisation, Environment framework, and Technology Threat Avoidance Theory were used to develop the conceptual framework for this study. A web-based survey was sent to 126 participants who all interacted directly with the DHIS in the Tshwane District Healthcare Centres. Structural relationships between factors were investigated using correlation and multiple regressions. Of the eight hypotheses, three were found to be significant. Training, top management support, and the perceived ease of use of the DHIS software were found by the multiple regression analysis to relate to cyber-attack avoidance motivation. However, the multiple regression analysis rejected hypotheses with TTAT factors and perceived usefulness of the DHIS software. This was even though the descriptive statistics showed that participants overwhelmingly agreed the severity of cyber-attacks, the system's vulnerability to such attacks, the effectiveness of the prescribed policies and controls, and the usefulness of the District Health Information System were important. The findings of the study also showed that health data was at high risk from ransomware attacks, phishing, and denial-of-service. Based on these findings, the threat of cyber-attacks results from the healthcare institutions' lack of suitable training, including for cyber-security personnel, and financial and other support from the organisation. The need to protect valuable data from hackers is crucial. Therefore, this research is essential for healthcare professionals, academics and researchers. Hence it is also valuable to the healthcare institutions in Tshwane District Healthcare Centres. This effectiveness will only be achieved if there is appropriate behavioural change on the part of those who can protect the system. The outcome of this study may be used as a recommendation on how to motivate users of the DHIS to implement and adhere to cyber-security controls.

Keywords: Cyber-security, District Health Information System, healthcare centres, technology threat avoidance, Tshwane District

PUBLICATIONS

1. Netshishivhe, T. A., Chimbo, B., Motsi, L., Chiyangwa, T., & Alexander, P. M. (2023). Cyber-attack Avoidance Motivation of Health Information Systems users at district clinics in South Africa, (Provisionally accepted at the Electronic Journal of Information Systems in Developing Countries).
2. Netshishivhe, T. A., Chimbo, B., Motsi, L. (2023) Framework to mitigate cyber-attack avoidance on District health systems. (Under review at the South African Journal of Information Management).

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION	1
1.1 Introduction	1
1.2 Background of the study	2
1.3 Problem statement	2
1.4 Research aim and objectives	3
1.5 Research hypotheses	4
1.6 Research methodology and design	5
1.6.1 Research paradigm, research philosophy and theoretical perspective	6
1.6.2 Research approaches	7
1.6.3 Data collection procedures	8
1.6.4 Data analysis	8
1.7 Validity and reliability	9
1.8 Ethical consideration	9
1.9 Significance of the study	10
1.10 Structure of the dissertation	11
1.11 Summary	13
CHAPTER 2: LITERATURE REVIEW	14
2.1 Introduction	14
2.2 Overview of cyber-attacks	14
2.3 The evolution of cyber-crime	15
2.4 Adoption of e-health technologies and cyber-security controls	16
2.5 Cyber-security and the healthcare sector	17
2.6 Current threats facing the healthcare sector	17
2.6.1 Cyber-attacks in healthcare: Global incidents	18
2.6.2 Cyber-attacks in the South African healthcare system	22
2.6.3 Cyber-attacks in healthcare during the COVID-19 pandemic	23
2.7 Vulnerabilities due to cyber-attacks	24
2.8 The impact of cyber-attacks on patients	25
2.9 Cyber-security legislation and frameworks	26
2.10 Cyber-security controls	29
2.10.1 Types of security control	29
2.10.2 Cyber-security control functions	30
2.11 Chapter Summary	30
CHAPTER 3: THEORETICAL FRAMEWORK	32
3.1 Introduction	32
3.2 Related theories	32
3.2.1 Social Cognitive Theory	32
3.2.2 System-Theoretic Accident Model and Processes model	34
3.2.3 Game Theory	35
3.2.4 Protection Motivation Theory (PMT)	36
3.3 Theoretical foundations	39
3.3.1 Technology, Organization, and Environment (TOE) framework	40
3.3.2 Technology Acceptance Model (TAM)	43

3.3.3	Technology Threat Avoidance Theory (TTAT)	45
3.4	Conceptual research framework model and hypotheses	49
3.5	Research hypotheses	52
3.6	Conclusion	57

CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY 59

4.1	Introduction	59
4.2	Research design	59
4.2.1	Types of research design	61
4.3	Research Philosophy	63
4.3.1	Positivism	64
4.3.2	Interpretivism	65
4.3.3	Realism	66
4.4	Research paradigms	66
4.4.1	Ontology	66
4.4.2	Epistemology	67
4.4.3	Axiology	68
4.5	Objectivism and subjectivism Philosophical assumptions	69
4.6	Research approach	70
4.6.1	Quantitative research approach	71
4.6.2	Qualitative research approach	73
4.6.3	Mixed methods	74
4.7	Research strategy	75
4.7.1	Case study	75
4.7.2	Survey design	75
4.8	Time horizon	78
4.9	Research population	78
4.10	Sampling techniques and sample size	79
4.10.1	Probability sampling techniques	79
4.10.2	Non-probability sampling techniques	80
4.11	Data collection procedure	82
4.12	Data analysis	83
4.13	Validity and reliability	84
4.14	Research limitations	85
4.15	Ethical considerations	86
4.16	Sample size	88
4.17	Chapter Summary	89

CHAPTER 5: DATA ANALYSIS AND INTERPRETATION 90

5.1	Introduction	90
5.2	Response rate and data cleaning	90
5.3	Demographics analysis	90
5.4	Demographics: Information systems knowledge	94
5.5	Exploratory factor analysis (EFA) Validity	97
5.5.1	EFA Validity Test	97
5.5.2	KMO (Kaiser Meyer Olkin) and Bartlett's test	97
5.5.3	Communalities	98
5.5.4	Total Variance Explained	99
5.5.5	Factor Rotated Component Matrix ^a and Interpretation	100

5.6	Reliability test (Cronbach Alpha)	106
5.7	Descriptive statistics	111
5.8	Correlation Analysis	116
5.8.1	Correlations with Cyber-Attack Avoidance Motivation	120
5.8.2	Hypothesis testing based on correlations	121
5.9	Regression Analysis	122
5.9.1	Model Summary	123
5.9.2	ANOVA	124
5.9.3	Regression Coefficients of the factors	125
5.9.4	Hypotheses Testing	126
5.10	Discussion	127
5.11	Conclusion	129
CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS		131
6.1	Research Overview	131
6.2	Addressing the research problem	131
6.3	Addressing the research objectives and hypotheses	132
6.4	Summary of the conceptual research framework	138
6.4.1	The theoretical contribution of the study	138
6.4.2	The methodological contribution of the study	139
6.4.3	The practical contribution of the study	140
6.5	Limitations of this study	140
6.6	Future research	141
6.7	Recommendations	141
6.8	Conclusion	143
APPENDICES		157
Appendix A: Gauteng Province Health Ethical Clearance Approval		157
Appendix B: Tshwane research committee Ethical Clearance Approval		158
Appendix C: UNISA Ethical Clearance Approval		159
Appendix D: Participant information sheet		162
Appendix E: Questionnaire		166
Appendix F: Editor's certificate		173
Appendix G: Turnitin Report		174

LIST OF FIGURES

Figure 1. 1 Dissertation structure	13
Figure 3.1 Social Cognitive Theory adopted from Bandura (1988)	33
Figure 3.2 Protection Motivation Theory (Rogers, 1975)	36
Figure 3.3 Technology-Organization-Environment Framework (Tornatzky and Fleischer, 1990)	40
Figure 3.4 Technology Acceptance Model (Davis, 1989)	43
Figure 3.5 Technology Threat Avoidance Model (adapted from Khan, 2017)	46
Figure 3.6 Conceptual Framework	51
Figure 3.7 Conceptual Framework Including Hypotheses	53
Figure 5. 1 Gender	91
Figure 5. 2 Age group	92
Figure 5. 3 Highest Education	92
Figure 5. 4 Positions	93
Figure 5. 5 Internet usage	94
Figure 5. 6 Password change	95
Figure 5. 7 Scree Plot	105
Figure 5. 8 Bar Chart of Responses Regarding Self-Efficacy	113
Figure 5. 9 Bar Chart of Responses for Training	114
Figure 5. 10 Bar Chart of Responses Regarding Top Management Support	115
Figure 5. 11 Conceptual Framework with Correlation	121
Figure 6.1 Final Conceptual Framework	139

LIST OF TABLES

Table 2.1: Global Incidents of Cyber-Attacks on Healthcare	19
Table 5.1: Demographics	91
Table 5.2: Information System Knowledge (Internet Usage)	94
Table 5.3: Information System Knowledge (Password Change)	95
Table 5.4: Information System Knowledge (General Questions)	95
Table 5.5: KMO and Bartlett's Test	97
Table 5.6: Communalities Test	98
Table 5.7: Total Variance Explained	99
Table 5.8: Rotated Component Matrix	101
Table 5.9: Cronbach's α Values Interpretation	107
Table 5.10: Reliability Factor of Technology Threat Avoidance Theory	108
Table 5.11: Technology, Organisation, Environment (TOE)	109
Table 5.12: Technology Acceptance Model	110
Table 5.13: Threat Avoidance Theory (TTAT) Factors	110
Table 5.14: Descriptive Statistics	111
Table 5.15: Correlation Statistics	117
Table 5.16: Hypothesis Testing using Correlation	122
Table 5.17: Model Summary	123
Table 5.18: ANOVA	124
Table 5.19: Coefficients	125
Table 5.20: Hypothesis Evaluation	126

List of Abbreviations

APT	Advanced Persistent Threat
CIS	Center for Internet Security
CSIR	Council for Scientific and Industrial Research
DHIS	District Health Information System
DoH	Department of Health
DOS	Denial-of-service
eHealth	Electronic-Health
EMR	Electronic Medical Record
HER	Electronic Health Record
HIS	Health Information system
HIT	Health Information Technology
HPCSA	Health Professional Council of South Africa
ICT	Information Communication Technology
ICT	Information Communication Technology
ICT	Information Communication Technology
IDSs	Intrusion detection systems
IoT	Internet of Things
IPSs	Intrusion prevention systems
ISO	International Organization for Standardization
ICT	Information Technology
KPMG	Klynveld Peat Marwick Goerdeler
MIT	Massachusetts Institute of Technology
NCPF	National Cyber-security Policy Framework
NIST	National Institute of Standards and Technology Cyber-security Framework
PMT	Protection Motivation Theory
TAM	Technology Acceptance Model
TOE	Technology, Organisation and Environment
UNISA	University of South Africa
WHO	World Health organisation

CHAPTER 1: INTRODUCTION

1.1 Introduction

The healthcare sector has changed dramatically since it was introduced to Information Communication Technologies (ICTs). According to Coventry and Branley (2018), technologically induced changes are the source of serious problems in the healthcare sector, such as data breaches and cyber-attacks. Consequently, cyber-security has become a significant concern for healthcare centres as they need to protect their data from cyber-criminals (Ahmed, Alsadoon, Prasad, Costadopoulos, Hoe & Elchoemi, 2017; Coventry & Branley, 2018). Ahmed et al. (2017) further note that cyber-criminals constantly develop new ways to attack systems, and therefore, businesses must also develop innovative and effective strategies to stop illegal access to information. Hospitals have slowly begun adopting and using technological advancements for better patient service using medical devices. Electronic health initiatives include the introduction of electronic health records, electronic prescriptions, and mobile health (Luna, Rhine, Myhra, Sullivan & Kruse, 2016). Khan, Serpanos and Shrobe (2018) note that hospitals deal with confidential information, including diagnosed diseases, personal demographic data and registration of births and deaths. These authors continue to point out that since the use of ICTs may expose this sensitive information to cyber-criminals, it is crucial to protect patients' interests.

This study aimed to determine the effective ways of encouraging compliance with the District Health Information System (DHIS) cyber-security controls by examining how healthcare support staff from the Tshwane District Healthcare Centres who interact directly with the DHIS perceive cyber-attack threats. Furthermore, by making use of several theoretical lenses, namely Technology Acceptance Model (TAM), Technology Threat Avoidance Theory (TTAT), and the Technology, Organization, and Environment (TOE) framework, the study examines how the DHIS users' security awareness levels aid in motivating technology avoidance behaviour. During the research undertaken for this dissertation, the people who completed the questionnaire were mainly from the following groups: Data capturers, Information clerks, IT Administrators, Heads of departments, Facility Information Officers, Facility Information managers, and District Information Managers. The staff at the healthcare centres who provide medical services at the Tshwane District Healthcare Centres do not generally interact directly with the DHIS.

1.2 Background of the study

Developments in technologies used in healthcare increase the quality of health service delivery at a lower cost and requiring less maintenance (Coventry & Branley, 2018). Furthermore, healthcare has been rated as a critical service industry due to the nature of the data they possess. According to Chenthara, Ahmed, Wang and Whittaker (2019) and separately Coventry and Branley (2018), healthcare information is both sensitive and valuable to certain people, and therefore hackers target these systems for the data they possess. Computer networks in healthcare centres are sometimes connected directly to medical devices, increasing systems' vulnerability (Camara, Peris-Lopez & Tapiador, 2015). Cyber-criminals can use healthcare data for identity theft, fraudulently obtaining a medical prescription, and unlawfully purchasing medical drugs to sell on the black market, and there are claims that ransoms are demanded to reinstate access to data and not corrupt databases (Coventry & Branley, 2018).

This data vulnerability was found by Coventry and Branley (2018) to be due to a lack of appropriate defensive cyber-security mechanisms and inadequate investments in cyber-security measures. The healthcare systems' lack of robust cyber-security defences makes them vulnerable to attacks and easy targets. Cyber-criminals are aware of this (Coventry & Branley, 2018). Healthcare service providers rely on data encryption, firewalls, and antivirus software to protect their ICT infrastructure. However, despite these measures, these systems remain very vulnerable to attacks via the Internet (cyber-attacks), including ransomware, denial-of-service attacks, phishing, and brute force or physical damage to medical equipment and electronic devices (Rajamäki & Nevmerzhitskaya, 2018; Coventry & Branley, 2018). These attacks endanger patients' lives, undermine trust, and make health information systems unusable (Coventry & Branley, 2018). According to Chenthara et al. (2019), 81% of health systems are vulnerable to cyber-attacks; this is clearly a serious concern. Therefore, the healthcare centres' apparent inability to reduce cyber-attack incidents is the main problem addressed by the researcher in this study.

1.3 Problem statement

The Mercury newspaper (2018), cited by Mapimele and Bokang (2019), reports that South Africa ranks third globally in cyber-crime, costing the country R2.2 billion annually. In addition, the frequency of cyber-attacks is increasing despite South Africa's implementation of

the Cyber-Crime Act 2017 (Department of Justice and Constitutional Development, 2017). Furthermore, hackers and cyber-criminals fully recognise the status of people interacting directly with the system as the weakest link in the security chain. These cyber-criminals routinely use social engineering tactics to trick users into installing malicious software (malware) or otherwise obviating technical security controls (Mitrovic, 2018). Tshwane District Healthcare Centres have already implemented the DHIS, and as this system runs on a networked computer system, it leads to exposure to cyber-attacks and cyber-threats (Camara et al., 2015). The security of the system is extremely important as any compromise of data, either due to lack of access to data, data loss, or data corruption, may lead to incorrect patient diagnoses, wrong patient treatment or, in the worst cases, can cause death. Cyber-criminals continuously take advantage of the poor security methods implemented in healthcare systems.

Healthcare has been seen to experience an extensive increase in data breaches, which has caused hospitals to lose money, suffer reputational damage and compromise patients' safety (Chiew, Yong, & Tan, 2018). According to (Djenna & Saïdouni, 2018), the healthcare industry has been listed as one of the most targeted sectors by cybercriminals lately. They stated in their paper that Vectra Networks conducted research, and their results show that healthcare is at the top of the list of highly affected industries due to the sensitivity of the data they possess (Djenna & Saïdouni, 2018). Furthermore, during the COVID-19 pandemic, the healthcare industry was most affected by cyber-attack (Davis, 2021). When cyber-criminals get a chance, they steal medical records, which may also cause damage or block healthcare services (Kruse, Frederick, Jacobson & Monticone, 2017). Given this reality, it is essential to understand how various users interacting directly with healthcare systems perceive and respond to information security risks (Mercury, 2018). Since limited research has been carried out in the area of cyber-attacks in the healthcare industry, it is not surprising that none has focused on the effectiveness of cyber-security controls on the DHIS in Tshwane District Healthcare Centres. Therefore, this study aims to fill the research gap by investigating the effectiveness of cyber-security controls in DHIS at Tshwane District Healthcare Centres.

1.4 Research aim and objectives

Published literature reports that if recommended methods to defend the system are not followed, health information systems become extremely vulnerable to viruses, malware, and ransomware (see Chapter 2). It is also proposed that if respondents can be motivated to comply

with cyber-security controls, they will change their behaviour accordingly and hence will contribute towards safeguarding the data and associated computer equipment (Liang & Xue, 2009). The underlying assumption made in this research is that cyber-security controls in the DHIS will only become fully effective as a means to prevent cyber-threats in healthcare centres if the people interacting with the DHIS are motivated to adhere to those controls and then consistently act in accordance with the prescribed processes and procedures.

Through an investigation of how healthcare support staff from the Tshwane District Healthcare Centres who interact directly with the DHIS perceive cyber-attacks, this study seeks to identify the most effective means of promoting compliance with the District Health Information System's (DHIS) cyber-security regulations.

The following specific research objectives were developed to achieve this goal:

1. To determine what cyber-attacks are common in the healthcare sector.
2. To assess what damage such attacks may cause at the healthcare centres.
3. To improve cyber-security of the DHIS by determining the current levels of knowledge of cyber-security policy, processes, and software by the users of the DHIS system and to what extent the respondents reported that they intend to carry out the required controls,
4. To improve cyber-security of the DHIS by determining what would motivate the users of the DHIS system to adhere more fully to cyber-security policy, processes and the use of software intended to detect and prevent breaches of the DHIS system.

These research objectives were answered by the data analysis and interpretation of the empirical research reported in Chapter 5.

1.5 Research hypotheses

In order to prevent cyber-attacks, an assessment was needed as to whether the staff perceptions of different motivating factors suggested by the literature encourage them to prevent cyber-threats in the DHIS.

Eight hypotheses were developed from the research objectives. This study seeks to test and validate the hypotheses listed below.

H1: Increased Perceived Severity has an increased positive impact on Cyber-attack Avoidance Motivation.

H2: Increased Perceived Susceptibility has an increased positive impact on Cyber-attack Avoidance Motivation.

H3: Increased Perceived Effectiveness has an increased positive impact on Cyber-attack Avoidance Motivation.

H4: Increased Self-efficacy has an increased positive impact on Cyber-attack Avoidance Motivation.

H5: Increased levels of Training have an increased positive impact on Cyber-attack Avoidance Motivation.

H6: Increased Top Management Support has an increased positive impact on Cyber-attack Avoidance Motivation.

H7: Increased levels of Perceived Ease of Use have an increased positive impact on Cyber-attack Avoidance Motivation.

H8: Increased levels of Perceived Usefulness have an increased positive impact on Cyber-attack Avoidance Motivation.

1.6 Research methodology and design

The following section outlines the research methodology and design that the study followed to solve the identified problem. According to Ranjit (2019), a research design is a procedural plan the researcher decides to follow to answer research questions adequately, precisely, objectively, and efficiently. Procedural plans are then translated from broad assumptions to precise step-by-step methods and strategies (Saunders, Lewis & Thornhill, 2019).

A survey strategy (see Section 4.7.2 in Chapter 4) was followed as is suitable for an explanatory study (see Section 4.2.1 in Chapter 4). The perceptions of the respondents regarding effective motivation were obtained using an online questionnaire. The quantitative data collected

indicated which factors¹ were considered to influence the attitudes of users of healthcare information systems to safeguard against cyber-attacks. With the aid of the study, the researcher was better able to comprehend underlying influences regarding human attitudes and consequent behaviour that exposes the DHIS to cyber-threats. This knowledge will assist IT managers in devising strategies to effectively protect the DHIS by increasing the acceptance of cyber-security controls. Therefore, this study sought to investigate and examine means for improving the effectiveness of cyber-security controls in the DHIS in the context of South African public healthcare, focusing on Tshwane District Healthcare Centres.

1.6.1 Research paradigm, research philosophy and theoretical perspective

A research paradigm is a set of values, norms and beliefs the researcher holds when conducting their study (Creswell & Creswell, 2018). Research philosophy is a belief in how data about a phenomenon should be collected, used, and analysed (Kivunja & Kuyini, 2017). Therefore, philosophy implicitly denotes the researcher's worldview (Kivunja & Kuyini, 2017). A worldview is the set of beliefs, perceptions, ideas, thoughts, or thinking that articulate the interpretation and meaning of research data. The positivist philosophical approach underpins this study. A positivist worldview is frequently applied when little to no understanding of a phenomenon exists. The researcher did not understand how adequate cyber-security controls to prevent cyber-attacks and associated strategies for encouraging compliance with them are in the DHIS. Therefore, understanding how to achieve compliance will improve the effectiveness of the DHIS cyber-security controls. The positivist philosophy was the appropriate choice for this study because it is rooted in the belief that there is a constant reality that can be defined objectively. This is because the social factors relating to the effectiveness of cyber-security control in DHIS are considered to be external to and hence unaffected by the researcher. In the context of this study, the positivist philosophy was accepted, and thus the quantitative approach was adopted so that reliable and valid conclusions could be derived.

A theoretical perspective is based on frameworks, theories and models that the researcher purposely chooses and integrates to develop a conceptual, theoretical framework. Integrating various theories forms a new theoretical framework that may be used in a research structure

¹ Throughout this dissertation the research elements are called factors rather than constructs.

that holds and shapes the study. This study integrated the following research frameworks and models:

- Technology Acceptance Model (TAM)
- Technology Threat Avoidance Theory (TTAT),
- Technology, Organisation, and Environment (TOE) framework

Protection Motivation Theory (PMT) is acknowledged as providing a major part of TTAT.

1.6.2 Research approaches

A research approach outlines the strategies and methods the researcher will use to collect, analyse, and interpret data to find new information (Creswell & Creswell, 2018). The approach outlines the methods and procedures used by the researcher to understand a phenomenon and address a research issue (Creswell & Creswell, 2018). This study followed the quantitative approach, allowing the researcher to statistically collect and analyse numerical data. According to Creswell and Creswell (2018), the quantitative approach tests the hypotheses by exploring relationships between variables. The data in these variables were obtained from research instrument, which was an online questionnaire, so analyses were done on numerical data using statistical procedures (Creswell & Creswell, 2018).

The study sought to determine whether cyber-security controls in the DHIS are likely to be effective by finding out which of the motivating factors the respondents perceive to be important. Furthermore, the study seeks to determine whether high levels of these motivating factors occurred when the respondents said they were highly motivated. In other words, the researcher sought to identify the strength of the relationships between the factors to confirm or refute the study's hypotheses.

A sufficiently large sample of participants was approached to collect the data that was used to find out which factors effectively motivate users to adhere to cyber-security controls. The researcher required feedback from a population of users who interact directly with the DHIS system. The staff at the healthcare centres who provide medical services at the Tshwane District Healthcare Centres do not generally interact directly with the DHIS. Therefore, the respondents were IT support staff and administrative staff. The chosen research method (a survey by means of online questionnaires) was helpful as it allowed easy access to participants, considering that

the necessary participants are always busy and at a variety of locations and are not easily accessible.

1.6.3 Data collection procedures

Researchers gather data from relevant sources to answer the identified research problems and questions, test hypotheses, and assess the outcomes (Creswell & Creswell, 2018). Primary data were collected to find out the perceptions of relevant staff members of the DHIS in the Tshwane district municipality regarding a number of factors related to cyber-security and their behavioural intention. In addition, data collected was used to evaluate whether users comply with cyber-security policies and controls for the DHIS used in the Tshwane district municipality. Primary data was collected using online questionnaires as a collection tool. The tool consisted of 21 compulsory and closed-ended questions that enabled the respondents to select the answer. A total of 160 participants were invited to participate in the study. 126 questionnaires were returned to the researcher. The target respondents in this study were from the following groups: Data capturers, Information clerks, IT Administrators, Heads of departments, Facility Information Officers, Facility Information Managers, and District Information Managers.

1.6.4 Data analysis

Data analysis is the process of reviewing, cleaning, transforming, and modelling data that has been collected (Ranjit, 2019). Collected data were analysed so that the researcher could fully comprehend what the findings indicated or meant. Demographic data were analysed using percentage and frequency distribution to get a general idea of who the respondents were. The data was analysed using the mean, standard deviation, and frequency distribution of descriptive statistics. Quantitative data analysis was done to determine the relationships between proposed motivating factors and the respondents' stated intention to comply with cyber-attack avoidance measures. Multilinear regression analysis was used to provide quantitative evidence of the effectiveness of cyber-security controls in DHIS. Statistical Package for the Social Sciences (SPSS) version 26.0 was used as a data analysis and presentation tool. SPSS is statistical software that provides advanced statistical analysis (Prusan, 2016). SPSS was used because it supports the top-down testing model of the hypotheses and is suitable for data analysis (Prusan, 2016).

1.7 Validity and reliability

The truth or reliability of findings is often discussed in terms related to the study's validity, and the conclusion must be sufficiently clear to answer the question that is stated in the research. Saunders et al. (2019) indicate that the validity of the measurement determines whether the instrument only measures what it is intended to measure. Therefore, content validity ensures that items match what is being evaluated.

Validity: Validity is known as the degree to which the tool can do what it is supposed to do, and that research questions really measure what they say they measure (Creswell & Creswell, 2018). In this study, content validity tests were applied to validate the sets of items of the data relating to each factor in the concept diagram. To increase validity, questions were based on the available literature and clearly related to the stated hypotheses and aim of the study. The researcher also considered whether findings could be generalized to larger populations and locations with similar characteristics to the study population as suggested or recommended (Saunders et al., 2019).

Reliability: The researcher concentrated on the stated research problem to find answers that addressed these concerns. In doing so, research design was found to be a critical tool in confirming whether the analysed data were reliable. Reliability of the approach that was used to measure data relies on the measurements (Ranjit, 2019). The instrument (questionnaire) that was used for measurements had to be able to provide reliable results every time it was used. Ranjit (2019) indicates that the reliability of a questionnaire is shown when participants understand the questions in a similar way, even at different times. Final results should not vary, except if there are differences in the variables that are being measured.

1.8 Ethical consideration

The researcher followed and adhered to the University of South Africa's (UNISA) research ethics policy to conduct the research responsibly and protect the rights of the research participants. Respondent's rights to anonymity, confidentiality and access to information were protected. Informed consent, harm protection, honesty, and the right to privacy are four ethical considerations discussed by Leedy and Ormrod (2005). Because humans were the focus or subject of the study, the researcher followed these categories to help draw attention to the ethical implications of what was planned. Permission to conduct the study was requested from

the Gauteng health department and Tshwane District Healthcare Centres. After permission was granted, invitations were extended to the participants. Only participants who gave consent were sent questionnaires, and there was no coercion or deception in participation in the study.

1.9 Significance of the study

This study's significance comes from addressing the main problem stated in the research. In order to prevent cyber-attacks, an assessment was needed of how respondents perceived the different motivating factors, which of these factors and to what extent they encourage the respondent to take cyber-security controls seriously, and then to what extent the respondents reported that they actually carried out the required controls. The main focus was whether highly motivated users apply cyber-security controls that protect the DHIS system at the healthcare centres of the Tshwane district municipality. Healthcare centres are vulnerable to different cyber-attacks; hence, this study was relevant (Zriqat & Altamimi, 2016). Therefore, the outcome of this research will contribute to the healthcare industry research by identifying effective cyber-security controls that can be used to prevent cyber-attacks in DHIS.

The practical significance of the research

This study is significant to healthcare professionals and researchers. It is valuable to the healthcare institutions known as Tshwane District Healthcare Centres. Implementing effective cyber-security controls in DHIS systems in South Africa will limit the number and severity of cyber-attacks that hospitals are exposed to, thereby protecting patients' data. The outcome of this study is a set of recommendations on implementing cyber-security control to reduce the occurrence of cyber-attacks. The study has generated new knowledge as it addressed the objectives stated in this chapter. The significance of this study, particularly within Tshwane district healthcare centres, is indicated below:

- The results of this study could help protect sensitive data from cyber-criminals, thereby saving lives by implementing effective controls that could prevent DHIS systems from being vulnerable to attacks.
- Furthermore, the findings may assist healthcare management in providing continuous and up-to-date information and training that will motivate end users to apply existing cyber-security controls that will prevent cyber-attacks on the DHIS system. The information and training will assist the users of the DHIS in identifying risks that the hospitals might be

exposed to and further implementing cyber-security controls enhancement measures at the Tshwane District Healthcare Centres.

- The research findings should benefit the health department and other stakeholders since the results offer guidelines for how the Tshwane District Healthcare Centres can successfully promote cyberattack avoidance behaviours in DHIS by fostering, observing, and assessing users' acceptance of cyber-security controls.
- The study's findings will enable district healthcare centres to coordinate their cyber-security measures in order to help them safeguard the privacy and safety of their patients. In addition, limiting disruptions that can have a detrimental impact on clinical results will assist in assuring the continuity of effective, high-quality care delivery.

1.10 Structure of the dissertation

The six chapters of the thesis are briefly outlined below:

Chapter 1: Introduction

This chapter briefly describes the nature of the threat to the South Africa e-health system at the Tshwane District Healthcare Centres. It provides the dissertation's organizational framework and contains the research background, the problem statement, the research aim and objectives, and the significance of the study. The chapter also briefly summarises the theoretical framework, research methods and design outline. Ethical considerations, validity and reliability of the study are discussed in this introductory chapter.

Chapter 2: Literature review

Chapter 2 includes a literature review describing the need for effective cyber-security controls in health information systems to prevent cyber-attacks. It also provides literature on cyber-threats affecting the medical sector and discussions on e-health. The chapter explored cyber-crimes, cyber-security controls and cyber-attacks in healthcare centres.

Chapter 3: Theoretical framework

This chapter presents literature related to Information Systems theoretical frameworks. The chapter gives a detailed discussion of the theories that underpin this study. Moreover,

research hypotheses are formulated, and operational definitions for each factor in the concept framework are presented. The results of this chapter and the extensive literature review in Chapter 2 contributed to accomplishing the study's objectives.

Chapter 4: Research design and methodology

In Chapter 4, the research methodology and design for the study are discussed in detail. The research approach, research design and research methods are also discussed. This chapter explains the sample size and population, study design, the questionnaire as a data collection tool, data analyses and how data will be analysed.

Chapter 5: Data analysis and interpretation

The data analysis and interpretation chapter focuses on the analysis and interpretation of the meanings of the data. This is achieved by using various analytical methods.

Chapter 6: Discussion, conclusion, and recommendations

This chapter includes what is recommended for future research, discussion and conclusions drawn from the results.

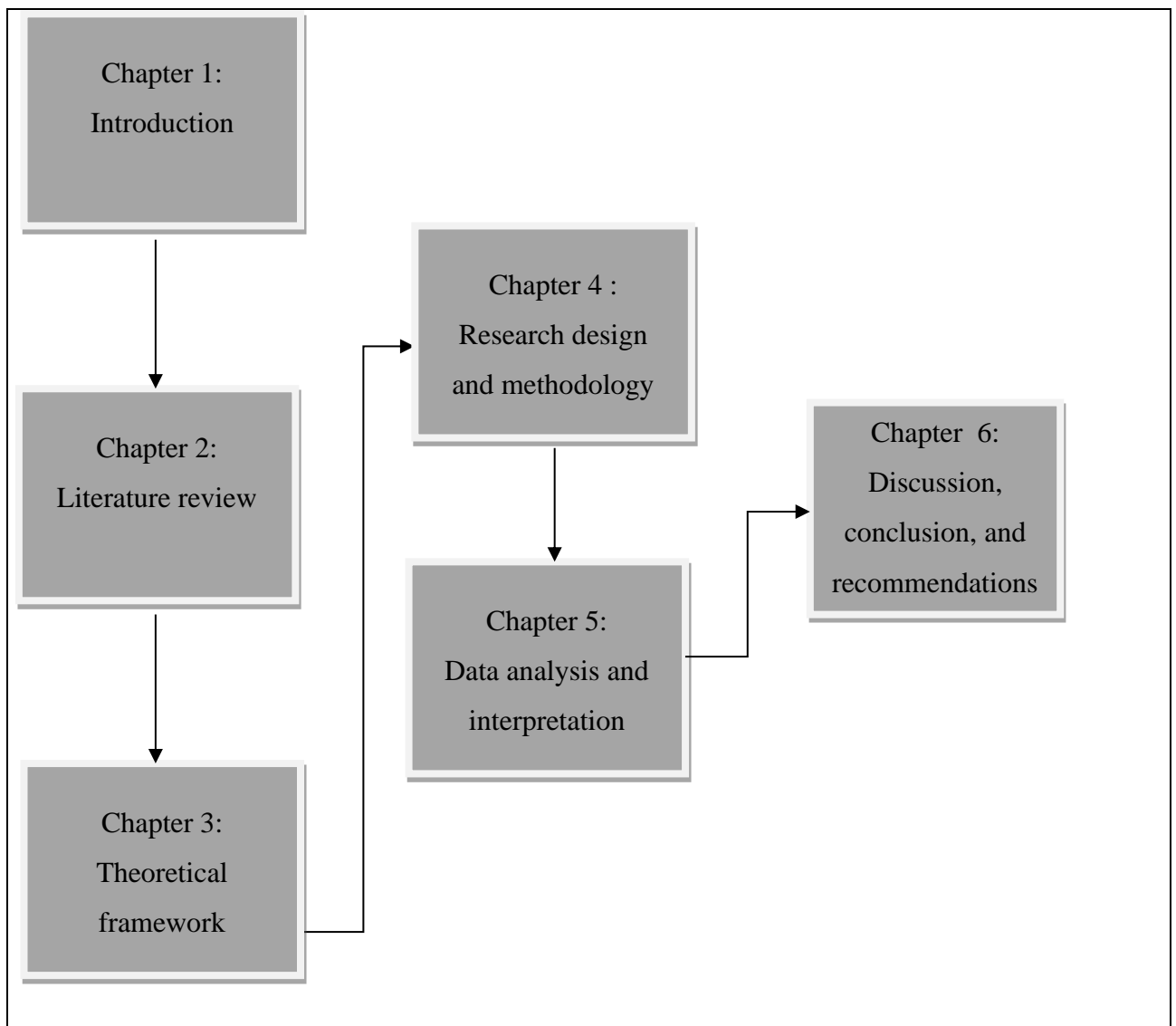


Figure 1. 1 Dissertation structure

1.11 Summary

The introductory chapter provided research background on the effectiveness of cyber-security controls in DHIS to prevent cyber-attacks. It provided a brief overview of the literature on cyber-attacks in healthcare centres and the theoretical foundations that underpin the study. Furthermore, the conceptual framework and research methods were also introduced. The next chapter contains the literature review.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter discusses literature reviewed relating to the ability of cyber-security controls in DHIS to prevent cyber-attacks. It starts by discussing cyber-crime and cyber-attacks in general before focussing on the cyber-threats affecting the medical sector and e-health. Cyber-security legislation and frameworks are described in the final section, cyber-security controls will be discussed, along with their various types and functions.

2.2 Overview of cyber-attacks

Fruhlinger (2020) defines a cyber-attack as the use of malicious code or malware with the intention of transferring it from one computer to many others via a computer network. These cyber-attacks are generally initiated by people whose goal is to cause the targeted computer or computers to malfunction or make them completely inaccessible via a network (Qamar, Karim & Chang, 2019). According to Kim, Kim and Park (2013), a cyber-attack is the intentional manipulation, using computing technology via computer networks, of systems owned by the targeted enterprises. Cyber-criminals use malicious code to modify computer code and data, causing disruptive effects that compromise computer data (Buch, Ganda, Kalola & Borad, 2017). These criminals gain access to computer systems by obtaining administrative rights and data through various nefarious means.

Cyber-attacks have become a growing criminal activity because cyber-criminals have seen that they are inexpensive to create and only need an Internet connection and a computer to implement (Buch et al., 2017). Furthermore, cyber-crime has a wide reach – it is unrestricted by distance and geographical location (Jang-Jaccard & Nepal, 2014). Another reason for the increase in this type of crime is that it is difficult to identify the persons behind the cyber-attack and to take legal action because the Internet has a nature of anonymity, and the criminals' location could be anywhere in the world (Buch et al., 2017). Due to this, cyber-attacks become more attractive to cyber-criminals, and the number of attacks is estimated to keep increasing. Jang-Jaccard and Nepal (2014) stated that cyber-attacks are estimated to cost billions of dollars each year. As a result, companies lose profits when they try to recover from cyber-attack. The increased dependence on technology by all kinds of enterprises is leading to cyber-attacks

being increasingly attractive, and its effects causing major disasters with increasing numbers of cyber-attack victims (Bendovschi, 2015).

Studies have shown that universally there is a lack of knowledge and understanding of cyber-attacks, their characteristics, and their effects on our lives (Bendovschi, 2015). This lack of understanding may hinder attempts to secure information systems. While different definitions of cyber-attacks exist, the aim is found to be common, which is compromising the availability, confidentiality, and integrity of data (Bendovschi, 2015). Cyber-attacks are a significant security threat and the biggest problem in ICT because attackers use various techniques and characteristics with different purposes (Bendovschi, 2015).

2.3 The evolution of cyber-crime

As technology advances, cyber-attacks evolve, and new approaches are developed (Qamar et al., 2019). Cyber-criminals modify existing malware codes to exploit new and existing technologies. New techniques are developed by cyber-criminals to find loopholes and install malware and hence to counteract the exclusive characteristics introduced when new technologies are designed (Jang-Jaccard & Nepal, 2014). Cyber-criminals quickly reach many victims since they take advantage of technology and gain access to billions of active Internet users. Victims are easily reached through smartphones, social media, critical infrastructure, and cloud computing (Buch et al., 2017). Technology evolution results in new cyber-crimes and brings about new forms of cyber-attacks that are difficult to identify and track. As a result, systems might be disrupted, and data can be compromised (Kim et al., 2013).

Hacking originated long before extensive networks of computers were created. College pranks were common on campus at the Massachusetts Institute of Technology (MIT), and these pranks were called hacks (Pavlik, 2017). MIT college students used to create pranks; for instance, building a replication or dummy police car and putting it on the university's roof (Pavlik, 2017). During the 1960s, the hacker concept changed from just being pranks that were created at MIT college to applications affecting the military (Ali, Samsuri, Seman, Brohi & Shah, 2018). Military data was stolen by cyber-criminals and sold to enemies (Ali et al., 2018). In this period, programmers were furious about this because the invention of computers was supposed to just make them live a better life (Pavlik, 2017). They believed computer information should be easily accessible and unrestricted (Pavlik, 2017).

In the 1970s, programmers developed telecommunication pranks, technology used to tamper with phones (Ali et al., 2018). Hackers used these 'phone phreaks' to gain free telephone calls or change phone ringtones (Ali et al., 2018). In 1971, Bob Thomas created a virus worm and named it "Creeper". This virus made the screen blank and displayed the text "*I'm the creeper; catch me if you can!*" (Matthews, 2019). The creeper virus resulted from an experiment by Thomas, who wanted to prove that he could develop a program that could replicate itself - he had no intention to harm (Matthews, 2019). In 1978, Carl Gartley and Gary Thuerk created the first e-mail spam (Sabillon, Cavaller, Cano & Serra-Ruiz.,2016). They developed an e-mail and sent it as spam using the Advanced Research Project Agency Network distribution list known as the ARPANET (Sabillon et al., 2016). In the 1980s, the virus known as Elk Cloner was developed by Rich Skrenta at the age of 15 (Buch et al., 2017). Elk Cloner was developed as a joke which was part of a game. However, the virus infected Apple computers as they booted-up with a floppy disk and replicated itself, thereby causing the screen to be blank (Thadani, 2013).

In 1986, Amjad Farooq Alvi and Basit Farooq Alvi created the first computer virus for the Microsoft Windows operating system and named it Brain (NortonLifeLock, 2020). The Brain virus was a boot sector virus that infected the floppy disk, replicated itself and displayed certain text when opened. These viruses were not harmful but annoyed people (NortonLifeLock, 2020). In 1988 Robert Morris Jr. released the first malicious program, originating from a computer at MIT, that was found on the Internet (Pavlik, 2017). The Morris worm was the first cyber-worm and spread at high-speed, resulting in computers stopping working. Within 24 hours, an estimated 6000 out of 60 000 computers connected to the Internet were hit and damaged by the Morris worm, which resulted in damage that caused about 98 million dollars for repairs (Pitts, 2017).

2.4 Adoption of e-health technologies and cyber-security controls

E-health is a way of improving healthcare services for everyone and requires the provision of critical infrastructure, which is the foundation for the exchange of information amongst health system users (Furusa & Coleman, 2018). E-health aims at delivering healthcare information and services online using related technologies at hospitals (Els & Cilliers, 2018). Therefore, e-health includes all parts of healthcare services that employ ICT to conduct diagnostics and implement technological advances and healthcare delivery improvements (Furusa & Coleman,

2018). E-health technologies also support campaigns to increase public awareness of health and medical issues. The use of technology to capture data and transmit information can reduce the number of medical record errors, promote quality healthcare, empower patients, and lower the financial burden on healthcare systems (Furusa & Coleman, 2018).

E-health adoption is becoming dominant worldwide, and these changes are leading to significant improvements to and even the transformation of service delivery and clinical outcomes. It signals a major change in the old, conventional healthcare systems (Furusa & Coleman, 2018). Nonetheless, protecting healthcare data and devices is becoming a major concern as technology advances (Coventry & Branley, 2018).

Computer networks and medical devices are interconnected, making them vulnerable to cyber-security breaches. Cyber-criminals are finding healthcare to be an attractive cyber-attack target because it contains valuable and critical data, and it usually does not have strong defences to fight cyber-crime. Cyber-security breaches that hospitals face include unauthorised access to health information, medical device attacks, and the demand for ransomware in hospitals. These attacks can lead to reduced patient trust, destroy health systems and threaten patients' lives (Coventry & Branley, 2018).

2.5 Cyber-security and the healthcare sector

Djenna and Sadouni (2018) list the healthcare sector as one of the fields most frequently targeted by cyber-criminals. This is due to the sensitivity of the healthcare data stored in their system. Research findings indicate that healthcare is at the top of the list of industries highly affected by cyber-attacks (Djenna & Sadouni, 2018). Three potentially harmful cyber-attacks in healthcare are session hijacking, ransomware, and denial-of-service attacks (Djenna & Sadouni, 2018). The following section discusses the cyber-threats that healthcare facilities are currently facing, cyber-attacks that have occurred in the South African and global healthcare sectors and incidents that have occurred amid the COVID-19 pandemic.

2.6 Current threats facing the healthcare sector

Cyber-criminals strive to access medical databases without authorization by using the real names of authorised medical professionals (Djenna & Sadouni, 2018). Consider a scenario where a data breach occurs at a hospital, and thieves steal patient records and, once in

possession of this data, a person's identity or insurance information might be used by someone else to unlawfully obtain healthcare services or prescription medications (Coventry & Branley, 2018). A full set of credentials for medical records stolen in this way is thought to be sold for more than \$1000 (Coventry & Branley, 2018). Selling prescription drugs on the dark web and claiming information that is susceptible to fraud have made cyber-criminals a lot of money (Coventry & Branley, 2018). Cyber-criminals may use data from medical records to open fictitious bank accounts, submit loan applications, or obtain passports (Coventry & Branley, 2018).

During a ransomware attack, hospital systems are blocked and encrypted, preventing authorised users from accessing the systems, the network is disrupted, and a denial-of-service attack brings down the system as a whole; patients suffer when hospital systems are rendered inaccessible for days or weeks at a time (Djenna & Sadouni, 2018). Bitcoin or another cryptocurrency is typically used to pay the ransom demanded by cyber-criminals (Djenna & Sadouni, 2018).

2.6.1 Cyber-attacks in healthcare: Global incidents

Many cyber- attacks targeting healthcare have occurred since 2014. Some of these are described briefly in Table 2.1, together with sources from which the information was obtained.

Table 2.1: Global Incidents of Cyber-Attacks on Healthcare

Date	Place	Type of attack and impact	Outcome	References
August 2012	The Surgeons of Lake County Hospital	Encrypted the data and demanded a ransom in return for the decryption key.	Not clear how much the hospital management paid in ransom or how they managed to get their systems back online.	(Paul III et al., 2018)
2014	Clay County Hospital in Flora	The hackers threatened to publish patients' medical records if a ransom demand of an undisclosed amount was not met.	Not clear how much the hospital management paid in ransom or how they managed to get their systems back online.	(Paul III et al., 2018)
5 February 2016	Hollywood Presbyterian Medical Center in Los Angeles, California	A ransomware attack; the system was not accessible to authorized personnel.	The hospital's CEO claimed that following negotiations, they paid the cyber-criminals a \$17,000 ransom because it was the quickest way to regain access to their system.	(Slayton, 2018) (Powderly, 2016) (Krisby, 2018)
No date	San Diego Hospital, located in Alvarado,	Ransomware attack: Once they had access to the hospital's computer, the hackers installed malware to encrypt the patients' data.	Management withheld information regarding which systems were impacted by the malware attack.	(Winton, 2016)
March 29, 2016	10 hospitals and more than 250 outpatient centres that are part of the MedStar Health chain Washington, DC.	Ransomware attack	Appointments were changed, and patients were transferred to other medical facilities because of the attack and some patient information was reported missing after restoring the system.	(Krisby, 2018) (Butt, Abbod, Lors, Jahankhani, Jamal & Kumar, 2019)
March 2016	Southeast Indiana's King's Daughters Hospital	Locky ransomware breach on a worker's file		(Miliard, 2016)
March 2016	Methodist Hospital in Henderson, Kentucky	Ransomware attack lasted for 5 days,	The system was eventually restored and no ransom was paid to the hackers.	(Krisby, 2018) (Monegain, 2016b)
May 2016	Kansas Heart Hospital	Ransomware attack - Samsam malware attack	The hospital paid the attackers demanded ransom, but despite receiving the money the attackers withheld all the hospital's data. The attackers then increased their ransom demand and the hospital refused to pay the second ransom demand no report details how the Kansas hospital handled	(Butt et al., 2019) (Siwicki, 2016)

			the circumstance.	
June 19, 2016	Professional Dermatology Care, based in Reston, Virginia	Ransomware attack accessed private financial and health information of 13237 patients and encrypted the patient data.	Demanded a ransom of an undisclosed sum.	(Davis, 2016a)
July 26, 2016	Greenbrae, California, Marine Healthcare District	This cyber-attack significantly impacted patients.	The hospital management informed the FBI, local law enforcement, and the Department of Health and Human Services. Investigations revealed that the vendor who provided the healthcare with an electronic medical record system and a medical billing system was responsible for the cyber-attack. The hospital paid the ransom demanded by cyber-criminals to get their system back.	(Davis, 2016c)
July 26, 2016	New Jersey Spine Center in Chatham	Ransomware attack	Resulted in a ransom payment to cyber-criminals.	(Davis, 2016c)
August 2016	The University of Southern California's two hospitals	The attack encrypted data that was saved on the hospital's servers.	The cyber-attack was contained to stop it from spreading to other computers.	(Monegain, 2016c)
August 2016	the urgent care centre in Mississippi, Oxford	Malware attack significantly slowed down the server. A ransom demand.	Clinic had to turn off its systems until the problem was fixed.	(Davis, 2016b)
No date	Ottawa Hospital in Canada	Ransomware attack	Only affected 4 computers - 9,800 uninfected computers the patient's information was secure.	(McCarthy, 2016)
April 9, 2017	Erie Country Medical Center Buffalo, New York	Samsam ransomware		(Wirth, 2018)
No date	One of the largest healthcare facilities in New York	Samsam ransomware: About 6000 computers were encrypted, forcing the hospital to manually handle patient care, The hospital chose not to contact the hackers used manual to restore backups, but this attack destroyed the online backup.	The hackers demanded a \$40,000 Bitcoin ransom. The system restoration cost them about \$10 million, and it took them six weeks to return to normal operations.	(Grossman, 2020) (CBS-NEWS, 2017) (Wirth, 2018)
May 12, 2017	A global cyber-attack impact on 100 nations	WannaCry ransomware, Investigations revealed that the Internet and other networks were used to spread the WannaCry attack,		Morse (2017) (Paul III et al., 2018)
2017	National Health	WannaCry ransomware resulted in	Shut down their system to stop WannaCry from continuing	(Coventry &

	Services (NHS) of the United Kingdom	device lockdown and blocked access to its systems, including e-mail correspondence 80 trusts 603 primary healthcare organizations and 595 general practitioners were severely impacted	to encrypt the other systems.	Branley, 2018) (Morse, 2017) (Wirth, 2018
January 11, 2018	1 Hospital	Samsam ransomware hackers used a vendor's login information to remotely access the hospital network	The criminals sought the decryption key in exchange for a ransom, the encrypted data was scheduled to be permanently deleted after seven days and it would be sold using Bitcoin on the dark web. However, it cost the hospital only \$55,000, and it took four days to decrypt the entire system.	(Wirth, 2018) (Berkeley & Gurdus, 2018)
September 27, 2020	One of the largest health systems in the United States, Universal Health Services	Caused 400 systems to go offline; had to use a manual system until system restoration, which took eight days to finish. During the outage, user access was suspended to all ICT systems and applications.	Resolved after three weeks.	(Dyrda, 2020)
October 28, 2020.	University of Vermont Health	Had a negative impact on 5000 computer systems. For at least 40 days, users were unable to access the system.	Lost about \$1.5 million per day between the cost of recovering the system and lost revenue.	(Dyrda, 2020)
October 26, 2020	3 hospitals	Ryuk ransomware attack: Within a day, this ransomware infected six hospitals in the United States.	Some hospitals that were impacted by it purchased new computers the ransom was paid.	(Roy & Chen, 2020)

2.6.2 Cyber-attacks in the South African healthcare system

It is claimed that most South African healthcare sectors have been affected by malware attacks but that hospital managers failed to report the majority of these instances (Van Niekerk, 2017). Cyber-criminals in South Africa have targeted private healthcare and hospitals since 2020 (Naik, 2021). In June 2020, while the country was fighting the Covid-19 pandemic, the Life Healthcare group in South Africa was a cyber-attack victim (Mungadze, 2020a). This group of hospitals is one of the country's largest private healthcare providers, with 66 healthcare facilities countrywide (Mungadze, 2020a). To contain the virus, their computer systems were turned off nationwide between June and the first week of July, and as the hospital system was completely inaccessible, the system's users were compelled to use pen and paper (Timeslive, 2020). The hospital was unable to process patient billing, create invoices for their suppliers, or process medical assistance claims and e-mail communication was also affected (Mungadze, 2020b). However, despite administrative bottlenecks and annoyances brought on by manual services, the Life hospital was still able to function (Timeslive, 2020). A manual backup system was used to restore the systems in July 2020 (Timeslive, 2020).

The 2020 Covid-19 pandemic was believed to have enabled cyber-attacks against several South African entities (Naik, 2021). This confirms the view that South Africa's healthcare facilities are amongst the most vulnerable to cyber-attacks globally (Van Niekerk, 2017). Recent research findings indicate that non-secured e-mail domains are used by South African healthcare facilities like clinics, laboratories, pharmacies, and medical practitioners, including hospitals (Naik, 2021). Computer forensics experts in South Africa have said that numerous hospitals have been victims of cyber-attack (Van Niekerk, 2017). However, they could not disclose the names of the hospitals affected since they signed non-disclosure agreements (Van Niekerk, 2017). It was discovered that during these attacks, criminals copy and store patient information, which can be used for later gains (Van Niekerk, 2017). This stolen patient's information can be published unlawfully online (Naik, 2021). In 2010, a state-owned hospital located in Western Cape was found to have a security Susceptibility where hackers could easily access the system (Van Niekerk, 2017).

2.6.3 Cyber-attacks in healthcare during the COVID-19 pandemic

According to Davis (2021a; 2021b):

- During the COVID-19 pandemic, there was a 45% increase in cyber-attacks worldwide against healthcare facilities, according to reports from Fortified Health Security and Check Point.
- Healthcare accounted for 79% of all reported cyber-attacks from the first ten months of 2020.
- The COVID-19 pandemic has impacted the healthcare industry the most. Denial-of-service attacks, remote code execution, botnets, malware, and ransomware attacks are some of the threats that are affecting the healthcare industry.
- Ransomware is considered to be the most dangerous cyber-threat to the healthcare industry.

A report that was released at the end of October 2020 reveals that a recent wave of ransomware attacks has affected US healthcare organizations (see Table 2.1). According to investigations, the Ryuk ransomware was the primary malware discovered in this attack (see Table 2.1). Cyber-attacks on healthcare organizations disrupt operations severely and put patients' lives in danger (see Table 2.1). Cyber-criminals are brutally targeting the healthcare sector since it is already under pressure and finding it difficult to deal with the COVID-19 outbreak. Service providers in the various parts of the medical sector are prone to paying ransom payments to secure patient data and bring their systems back up since healthcare systems are so complicated (see Table 2.1). An estimated 23.5 million patients have been cyber-attack victims during this period (Fortified, 2021).

Cyber-criminals gained access to the system for scheduling Covid-19 vaccination appointments at the Beaumont Internal Medicine Center in Southfield (Davis, 2021a; 2021b). The healthcare centre was compelled to shut down the system as a result of the attack. The electronic medical record system for Beaumont's immunization system exhibited some strange behaviours, according to the ICT department, and as a result, they turned off the system to control the virus (Davis, 2021a; 2021b).

Cyber-criminals gained access to the server containing vaccine data from pharmaceutical behemoths BioNTech and Pfizer in early December 2020 and released information about the COVID-19 vaccine (Davis, 2021a; 2021b). When hackers illegally published the data online, European medicine regulators learned about the cyber-attack (Davis, 2021a; 2021b). European Medicines was investigating the COVID-19 vaccine's evaluations and approvals at the time, as BioNTech and Pfizer had given their COVID-19 approvals data to the European regulators just before the system was attacked (Davis, 2021c). The hackers stole the documents by removing them from approval. The cyber-attack only affected one ICT system (Davis, 2021c).

2.7 Vulnerabilities due to cyber-attacks

Usually, hospitals have security patches (code to defend their systems and data), but they have not been installed in many cases. In 2017, an attack known as WannaCry (see Table 2.1) disrupted many different industries worldwide. Over 300,000 computers in about 100 different countries were infected by the WannaCry virus, which instructed users to pay a ransom in Bitcoin (Morse, 2017). The denial-of-service affected more than 50 hospital systems in the UK, causing delays in patient care and malfunctions with connected devices, including equipment used to store different types of blood, MRI scanners and refrigerators. Despite not exclusively targeting the medical sector, the WannaCry attack had a significant and widespread impact on many hospitals, clinics and other healthcare facilities (Morse, 2017). A ransomware virus was reported to have also attacked the National Health Services of the United Kingdom trust in 2016 (Coventry & Branley, 2018).

Following a significant ransom attack at the Hollywood Medical Center in Los Angeles, California, in February 2016, hackers began specifically targeting the healthcare industry (Ragan, 2016). This attack impacted the hospital and encrypted patient records; X-ray machines and other medical equipment broke down, making it impossible for staff to care for patients. The attackers had demanded a \$3.6 million ransom, but after negotiations, they settled for \$17,000. Cyber-criminals began targeting hospitals more frequently after this attack was successful because the ransom was paid; two hospitals were attacked in that month, and five hospitals were attacked the following month (Paul III et al., 2018).

Other virus outbreaks have resulted in significant breakdowns. For instance, a healthcare trust in the UK experienced an undisclosed attack that forced it to close its ICT systems, suspend operations, and cancel patient appointments for four days (see Table 2.1). Another attack affecting the healthcare industry is a "medical device hijack" or "MadJack attack." All devices connected to the hospital network are affected by this MadJack attack, which spreads malware into unprotected medical devices (Paul III et al., 2018).

2.8 The impact of cyber-attacks on patients

The introduction of the Internet and the associated integration of information and communication technologies has increased the Susceptibility of healthcare systems to cyber-attacks (Dogaru & Dumitrache, 2017). As noted earlier, these vital systems are susceptible to identity theft, unauthorized access to lab reports, disruptive attacks, and loss of medical data stored in databases.

A security breach may result in incorrect health decisions for patients, and being unable to use medical devices connected to the network may result in death (Dogaru & Dumitrache, 2017). Following an investigation, the NHS found that approximately 1220 pieces of diagnostic equipment were infected by the WannaCry ransomware during the global WannaCry attack (Morse, 2017). Medical workers were unable to use tools like MRI scanners as a result. Because the systems were not available, patients who were due to be discharged were kept in hospital because medical professionals lacked appropriate knowledge of which patients needed what (Morse, 2017).

Turning off all computer systems until it is safe to turn them back on stops the virus from spreading but during this pause hospitals must manually maintain patient records (Miliard, 2016; Williams, 2016). However sometimes hospital ICT administrators are not the people make the decision as cyber-criminals lock their systems (Reynolds, 2021). The loss of access to ICT systems affects the admissions process, e-mail communication including e-mails containing medical images and reports, and business processes (Reynolds, 2021). In addition, hospitals lose money when they are forced to close due to cyber-attacks (Sparrell, 2019). Patients' appointments have to be rescheduled or are simply cancelled, and new patients

entering hospitals may be routed to other hospitals because of the systems' unavailability (Coventry & Branley, 2018).

Patients are negatively affected when cyber-criminals reveal their private and sensitive information to others, especially medically sensitive information (Coventry & Branley, 2018). They become reluctant to provide the doctors with their personal information due to this risk. Medical data exposure is a severe problem, especially when it comes to stigmatized disorders and sexually transmitted diseases like HIV (Coventry & Branley, 2018).

2.9 Cyber-security legislation and frameworks

The following section discusses the cyber-security legislation and frameworks that guide the cyber-security best practices and standards to help combat cyber-attacks and vulnerabilities in the context of South Africa. The National Cyber-security Policy Framework (NCPF), the Cyber-Security and Cyber-Crime Bill and The Protection of Personal Information Act (POPIA) were discussed.

National Cyber-security Policy Framework

National governments have challenges relating to data protection and need to coordinate cyber-security strategies in all government spheres and between private entities, small businesses, and individuals. During 2015, the Minister of State Security of South Africa implemented the National Cyber-security Policy Framework (NCPF) to address the challenge.

"The purpose of the NCPF is to create a secure, dependable, reliable and trustworthy cyber-environment that facilitates the protection of critical infrastructure whilst strengthening shared human values and understanding of cyber-security in support of national security imperatives and economy" (Minister of State Security, 2015)

The NCPF allows the development of an information society that safeguards the essential rights (dignity, freedom of expression, security, communication rights, access to information rights, and security) of South African citizens (Minister of State Security, 2015). This framework strives to ensure that the cyber-space is secure and assures civil society, businesses, and government entities that they can use it freely.

National governments need to adopt cyber-security strategies to address cyber-threats such as ransomware, identity theft, denial-of-service, cyber-bullying, and other acts of crime in cyberspace (Jideani, Leenen, Alexander & Barnes et al., 2018).

The Cyber-Crime and Cyber-Security Bill

The Cyber-Security and Cyber-Crime Bill was created to address cyber-crime in South Africa, and if the offences covered by the bill are committed, the bill will help enforce penalties (Mangena, 2016). The bill ensures that temporary restraining orders may be obtained against anyone who distributes data transmitted illegally (Sutherland, 2017). It requires that investigations into cyber-crime are conducted in cooperation with all stakeholders (Mabunda, 2019). It means that cyber-crime victims have a point of contact that is available around the clock. Affidavits can also be used to provide information about cyber-crime (Sutherland, 2017). Financial institutions and providers of electronic communication services are required to report cyber-crime and to cooperate with authorities in their investigations (Mabunda, 2019).

The Cyber-Crime and Cyber-Security Bill has identified a list of crimes which are regarded as criminal offences, and these are:

- Unlawful securing of access to data
- Unlawful acquisition of data
- Unlawful acts in respect of software or hardware tools
- Unlawful interference with data or computer programs
- Unlawful interference with a computer data storage medium or computer system
- Unlawful acquisition, possession, provision, receipt, or use of a password, access codes, or similar data or devices
- Cyber-fraud
- Cyber-forgery and uttering
- Cyber-extortion
- Malicious communication
- Data message which incites damage to property or violence
- Data message which is harmful

- Distribution of data message of an intimate image without consent (Minister of Justice and Correctional services, 2016)

South African data protection: the POPI Act

The Protection of Personal Information Act (POPIA) No. 4 was adopted and put into effect by South Africa on November 19, 2013. (Department of Justice and Constitutional Development, 2018). This legislation aims to safeguard the private and public sectors' collection and processing of individual personal information as well as to ensure Act compliance (Iyamu & Ngqame, 2017). The lack of privacy legislation in the nation, which would have protected how personal information is processed, collected, transferred, and stored, led to the adoption of this legislation (Taplin, 2021). Basic privacy laws are in place in South Africa, but POPIA provides an additional layer of protection as it is increasingly challenging to ensure personal safety in the technological age (Kandeh Botha & Fitcher, 2018). The Act will accomplish this by establishing a strict personal data protection policy and enforcing it against those who collect and process personal data (Shanapinda, 2019). It adheres to international standards for regulating and overseeing legal procedures for collecting and processing personal information (Shanapinda, 2019).

Furthermore, POPIA outlines how individuals can protect their personal information and their legal rights (Batchelor & Wazvaremhaka, 2019). An associated regulatory body was selected and appointed by the President of South Africa in December 2016 (Batchelor & Wazvaremhaka, 2019). This regulatory organization aids in the enforcement of POPIA to protect personal data. In addition, the regulating agency states that people who violate POPIA may also be subject to a ZAR10 million fine, 10 years in prison, or both (Shanapinda, 2019). POPIA was enforced in July 2021 to counter illegal actions after it officially went into effect on July 1, 2020 (Iyamu & Ngqame, 2017). The POPIA imposes eight obligations related to the lawful collection, use, disclosure, processing, and storage of personal information (Iyamu & Ngqame, 2017). These include accountability, restrictions on processing, information quality, transparency, security measures, and data subject participation (Department of Justice and Constitutional Development, 2018).

2.10 Cyber-security controls

A cyber-security control is anything that reduces risks related to the transmission or storage of data by an industry or organisation (Silva, Ferraz, Guelfi, Barboza & Kofuji, 2019). Usually, these are activated as a response to threatening experiences or incidents. These typically occur not because there are no controls in place but rather because the controls that were in place were inadequate. Making sure that implemented controls are effective is, therefore, crucial in control management (Silva et al., 2019). Controls for cyber-security are divided into control types and control functions. Examples of cyber-security control types are physical, technical, and administrative controls. Prevention, detection, and corrective controls are types of cyber-security controls discussed briefly below.

2.10.1 Types of security control

Physical controls protect things that you can touch, such as assets, physical areas, systems, or computers (You, Lee, Oh & Lee, 2018). They are intended to discover or prevent unauthorised access. Examples include security badges, lighting, gates, surveillance cameras, biometric access controls, fences, motion sensors, access cards, guards, and surveillance cameras (You & Lee, 2018). These are clearly not all directly computer based but nevertheless assist in preventing access to information systems, data and computer hardware.

Technical or logical controls are software or hardware mechanisms that safeguard assets (Marjanovic, 2013). These include software that covers authentication, antivirus protection, firewall protection and protection from intrusions, such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (Marjanovic, 2013).

Administrative controls are used to define the practice of business or personnel following the security goal and objectives of the organisation and are achieved by developing procedures, policies, and guidelines that must be followed to protect the security of the organisation (Such, Vidler, Seabrook & Rashid, 2015).

2.10.2 Cyber-security control functions

Preventative controls are developed to prevent activities that are not authorised, such as locks, alarm systems, or fences for physical control protection and firewalls or antivirus prevention software and classification of data or duties separation for administration control protections (Wanyonyi, Rodrigues, Abeka & Ogara, 2017).

Cyber-security detective controls are measures implemented so that they can detect and inform administrators about access or activities that are not authorised or that are not wanted when they occur or shortly after they have occurred (Dibaji, Pirani, Flamholz, Annaswamy, Johansson & Chakraborty., 2019). These are physical controls such as physical sensors and alarms and technical controls such as IDS (Dibaji et al., 2019).

Cyber-security corrective controls are used for damage control to restore the capabilities and resources of a system to its previous state after unauthorised activity has occurred (Wanyonyi et al., 2017). Rebooting a system or data restoration is an example of technical corrective cyber-security controls, and a response team is another control (Wanyonyi et al., 2017).

2.11 Chapter Summary

In this chapter, it is noted that the widespread introduction of information and communication technologies into the medical sector and the rapidly evolving nature of this technology are amongst the factors that have made the sector attractive to cyber-criminals. Furthermore, the medical sector is highly dependent on patient data as part of planning and providing patient treatment and for organisational processes. This makes the sector as a whole, and patients in particular, extremely vulnerable to the threats related to cyber-attacks. Maintaining the integrity of healthcare data and its privacy is essential.

The effectiveness of cyber-security depends on processes, people, and technologies that safeguard investments in technologies and digital data. Hackers continually discover new ways to attack the enhanced cyber-threat defence mechanisms; therefore, it is a constant battle. Healthcare organisations often implement technologies with no proper cyber-security controls, making them easy targets. Hospitals transmit more and more data electronically using medical devices, mobile technologies, cloud technologies, and technology infrastructures.

Following the ransomware attacks that targeted hospitals in the United States in 2016, which were widely reported, cyber-criminals began specifically targeting healthcare. The fact that ransom payments were made encouraged criminals to rapidly launch an escalating number of attacks on hospitals. The chapter presented a timeline showing details of some of the attacks made on healthcare facilities worldwide, cyber-attacks that have occurred in South Africa and incidents that have occurred amid the COVID-19 pandemic. The most common types of cyber-attacks are session hijacking, ransomware, and denial-of-service attacks.

This chapter also discussed existing controls that assist in cyber-security. These include legislation and some examples of types of cyber-security controls and their functions. Hence this chapter has answered the first two research objectives by referring to the literature, namely:

1. what cyber-attacks are common in the healthcare sector,
2. what damage such attacks may cause at the healthcare centres.

Chapter 3 will provide a theoretical basis for the conceptual model used in the empirical part of this research. This will be used in developing the hypotheses.

CHAPTER 3: THEORETICAL FRAMEWORK

3.1 Introduction

This study developed a conceptual framework to evaluate how effectively the DHIS cyber-security measures in Tshwane District Healthcare Centres prevent cyber-attacks. Various frameworks adopted from Information Systems (IS) theories were integrated to develop this framework. This chapter considers several theories related to the study, namely Game Theory, Social Cognitive Theory, the System-Theoretic Accident Model and Processes (STAMP) and Protection Motivation Theory (PMT). However, these theories were not used in developing the conceptual framework due to some limitations that were identified. Instead, the underpinning theories for this study are Technology Acceptance Model (TAM), Technology, Organisation, Environment (TOE), and Technology Threat Avoidance Theory (TTAT), which are also discussed. A justification for the decision as to which theories to incorporate (the reasons and the relevance of adopting these frameworks) was also given.

3.2 Related theories

This section discusses some of the IS theories that are relevant to this research. Social Cognitive Theory, System-Theoretic Accident Model, and Game Theory have been extensively applied in other academic studies; however, they were found not suitable for this study, and the reasons for their unsuitability are discussed below.

3.2.1 Social Cognitive Theory

Social Learning Theory is the formal name for Social Cognitive Theory (SCT) and was created for and is widely used in research in communication and psychology (Bandura, 1988). Extensive research in these fields means that SCT has been validated and hence is recognised as a means of understanding, altering, and forecasting how people act in groups and individually (Bandura, 1988). According to Bandura, SCT shows that a person's behaviour is related to their environment, personal circumstances, and behaviour (1977, 1986). SCT proposes a model for changing, understanding, and predicting humans behaviour. It is applicable to groups of people and individuals and can help researchers to predict how groups

and individuals will behave or understand how they have behaved previously (Bandura, 1988). Therefore, procedures for modifying or changing behaviours can be developed using SCT (Bandura, 1988). Bandura (1988) explains the factors represented in SCT, namely behavioural (b) factors, personal (P) factors in the form of cognitive, effective, and biological events, and the external environment (E). Social Cognitive Theory is depicted in Figure 3.1 below.

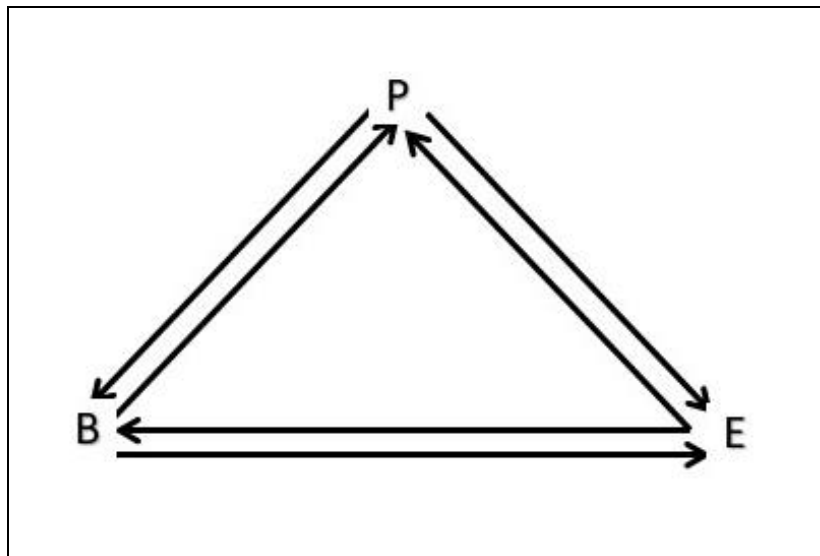


Figure 3.1: Social Cognitive Theory adopted from Bandura (1988)

Limitations of Social Cognitive Theory

Social Cognitive Theory (SCT) was considered unsuitable for this study. The theory is based on a framework to help understand and predict human behaviour (Bandura, 1988). Relationships between the three factors are central to SCT, such as a change in the environment leads to a change in human behaviour, but this is not always the case (Bandura, 1988). Another assumption underpinning SCT is that behaviour is learned primarily through observation, reinforcement, and expectations. SCT does not allow for the fact that people can change their behaviour dramatically due to experiences encountered as they progress through life, even though there has been little or no environmental change (Bandura, 1988). In SCT, there is minimal attention to the importance of motivation and emotions and no reference to experience. Despite being a well-respected theory, the theory cannot allay concerns regarding DHIS cyber-attacks.

3.2.2 System-Theoretic Accident Model and Processes model

The System-Theoretic Accident Model and Processes (STAMP) framework was developed to pinpoint key ideas behind an accident (Salim & Madnick, 2016). However, understanding why accidents happen requires an analysis of why existing controls were ineffective (Salim & Madnick, 2016). STAMP does not concentrate on preventing incidents but instead focuses on developing effective controls with the aim of applying restrictions relevant to the system. The major concepts of the STAMP model are safety constraints, a process model, and hierarchical safety control (Salim & Madnick, 2016). STAMP uses CAST (causal analyses based on STAMP) to analyse incidents and has been used to analyse cyber-attacks for cyber-security. The purpose of CAST is to completely comprehend why the incident happened (Salim & Madnick, 2016). Therefore, it analyses incidents within sociotechnical systems holistically so that there is a full understanding of causal factors that occurred randomly or systematically. Furthermore, it assists in comprehending the reasons that loss occurred, and it develops further measures to avoid incidents that might happen in the future (Salim & Madnick, 2016).

Limitations of System-Theoretic Accident Model and Processes

The limitation of STAMP is that it does not necessarily prevent attacks on the system and hence does not assist in developing comprehensive system engineering methodologies to prevent incidents. Common causes of accident factors are ignored in this theory (Salim & Madnick, 2016). It also makes assumptions that incidents often occur randomly as events come together accidentally. In STAMP, the incidents it studies are only because of a lack of control (accidents) and not a result of a series of planned events (Salim & Madnick, 2016).

Despite the fact that STAMP has been used in some recent research into cyber-security in the medical sector (Salim & Madnick, 2016; Askar, 2019), it was not considered to be appropriate to this study because its primary purpose is to analyse why the accident happened by focusing on why the control was ineffective. Identifying fundamental reasons for accidents is difficult in today's increasingly complex systems with various interacting aspects. Instead of viewing incidents as the result of an initiating (root cause) event in a series of events leading to a loss (an accident), malevolent incidents result from interaction among components that violate the system safety constraints (Salim & Madnick, 2016).

3.2.3 Game Theory

Game Theory models the strategic interaction between two or more players in a situation containing a set of rules and outcomes and, hence, focus on studying relationships between decision-makers (Nissan, Roughgarden, Tardos & Vazirani, 2007). Players make decisions in a setting where they strategically interact with a game. The choices made by a player could benefit the other player and vice versa (Nissan et al., 2007). Predictions, actual behaviour, and the methods players employ are investigated using Game Theory (Nissan et al., 2007).

Within the same game, different situations may rely on the same incentive structures. In contrast, a game can be played more than once by the same people and nevertheless yield different results depending on their strategies during the different game events (Nissan et al., 2007). Game Theory has played a significant role in computer science and logic. As a result, many logic theories have been developed based on Game Theory (Van Dijk, Juels, Oprea & Rivest, 2013). Academics from computer science make use of games to construct interactive computational models (Van Dijk et al., 2013). Of course, Game Theory is also, particularly of interest in designing computer games and creating highly effective computer-based players to act as competitors for people playing traditional, rule-based games like chess online.

Limitation of Game Theory

Game Theory has multi-agent system theoretical foundations (Shoham, 2008). According to Van Dijk et al. (2013), Game Theory effectively constructs models that interact with both intelligent cyber-defenders and intelligent cyber-attackers. Therefore, in the cyber-security context, Game Theory is used to create tactics that effectively neutralise cyber-threats (Van Dijk et al., 2013). Similarly, Game Theory has been applied to developing security games intended to avoid assaults (Nissan et al., 2007).

A limitation of Game Theory is that it assumes that players interacting in a game assess a situation consistently and hence follow the same strategy at all times (Manshaei, Zhu, Alpcan, Baçşar & Hubaux, 2013). However, this can be shown not to be the case even when playing formal games like Chess or Bridge, as different players make different assessments and use different strategies; players can play the same game with the same resources and get different scores depending on an individual's strategy (Van Dijk et al., 2013).

The primary purpose of this theory, when related to cyber-attacks, is to try to predict whether the attacker will be able to penetrate the secured system (Manshaei et al., 2013). However, in the context of cyber-security, criminals do not play according to rules, and technology evolves. Hence the limitation noted above (following the same strategy at all times) is particularly serious. Therefore, ame Theory was judged irrelevant to this study.

3.2.4 Protection Motivation Theory (PMT)

Rogers proposed the Protection Motivation Theory (PMT) in 1975, which explains how fear motivates one to defend oneself to achieve health benefits (Chenoweth, Minch & Gattiker 2009). This widely accepted theory describes the cognitive processes resulting in behavioural changes (Biggsby & Albarracin, 2022; Chenoweth et al., 2009). This theory was initially developed to understand and predict people’s behaviour when responding to a variety of threats or fear (Zhao Cavusgil & Zhao, 2016). According to Witte (1992), a threat is an external stimulus that exists whether an individual is aware of it or not.

Figure 3-2 illustrates the components of the PMT model.

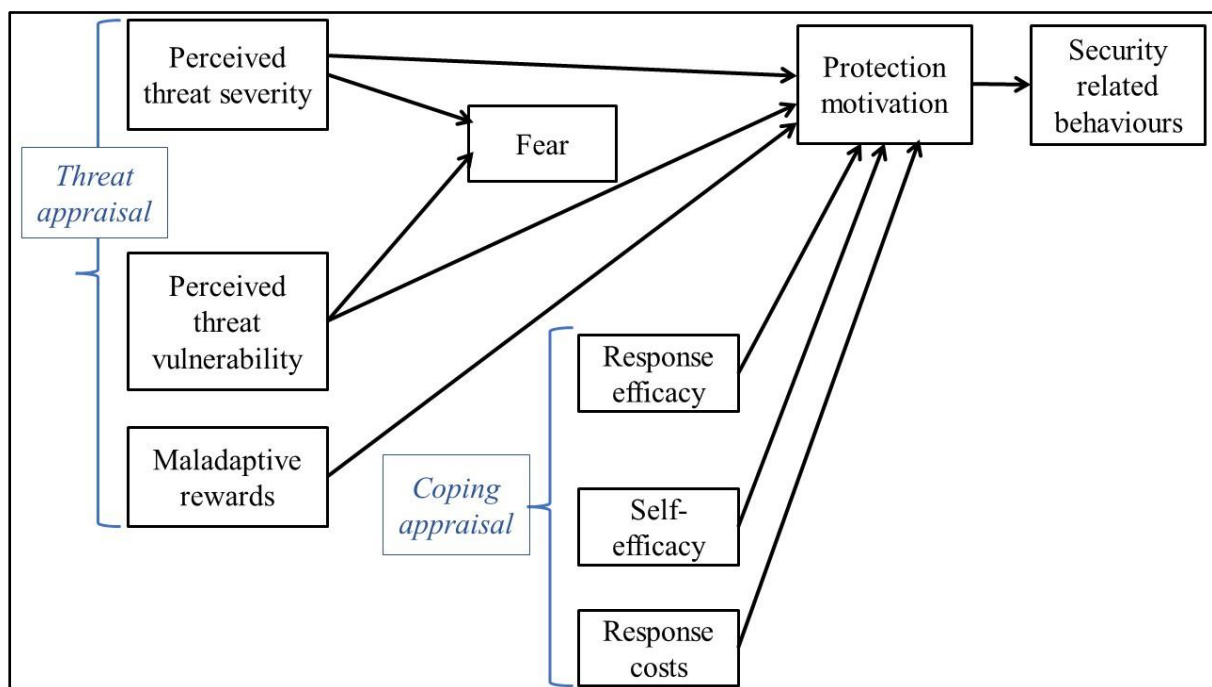


Figure 3.2: Protection Motivation Theory (Rogers, 1975)

Rogers created the most recent version of the PMT in 1983 to understand better how and why people react to potential health and safety threats (Clubb & Hinkle, 2015). Recently Tsai, Shih, Hsieh, Chen, Lin and Wu (2022) have added that PMT shows that individuals are motivated to participate in appropriate health behaviours to avoid health risks and gain interpersonal and social benefits.

Cognitive Process

Rogers focuses on the cognitive processes that come into play when people are faced with threats or harmful situations (Biggsby & Albarracin, 2022; Chenoweth et al., 2009). According to Vance, Siponen, and Pahlila (2012), if a person is aware of a threat, they evaluate the threat's intensity and likelihood that they would be directly impacted. If they believe they can cope with that threat, they are more likely to engage in protective measures (Menard, 2017). According to the PMT, when people are confronted with a threat, they go through a cognitive process, including threat appraisal and coping appraisal (Wu, 2020). Intentions to protect themselves are determined by the perceived cost of risk reduction behaviour (how difficult it will be) and the perceived benefits if the risk is opposed (how important it is to remain safe) (Menard, 2017).

Threat appraisal

Maddux and Rogers (1983) defined threat appraisal as the individual's judgment of threats arising from negative environmental changes are highlighted by fear appeals. The theory assumes that when people are faced with risky and threatening situations, they have a strong motivation to protect themselves from such threats (Chenoweth et al., 2009). An individual evaluates a threat (a) based on how severe the consequences will be (Perceived Threat Severity) (Anderson & Agarwal, 2010) and (b) on their own susceptibility to the threat and the likelihood that the risk will occur (Perceived Threat Susceptibility) (Biggsby & Albarracin, 2022; Clubb & Hinkle, 2015; Wu, 2020; Chenoweth et al., 2009). A belief of acute danger plus a belief that it is likely to occur will heighten the emotional response (fear) and influence the behaviour and attitude toward change (Biggsby & Albarracín, 2022).

It further explains that individuals are motivated to respond to cautions or warnings from others about threats or dangerous behaviours, known as fear appeals (Chenoweth et al., 2009). Fear

appeals urge people to cooperate by describing the negative things that will happen if they do not follow recommendations (Chenoweth et al., 2009). Fear appeals include notifications that a threat might exist but also suggest the individual is susceptible to that particular threat and the threat is severe (Anderson & Agarwal, 2010; Clubb & Hinkle, 2015). An individual can now decide how vulnerable they are to the threat (Menard, 2017; Zhao et al., 2016). Maladaptive behaviours are also examined in threat appraisal (Clubb & Hinkle, 2015). These are behaviours that are not 'correct', moral or suitable under the circumstances. Maladaptive rewards are what motivate someone not to seek protection from the threat. Therefore, as part of threat appraisal, the potential victim might identify some maladaptive reward for ignoring the threat (a maladaptive response) (Clubb & Hinkle, 2015). Maladaptive rewards can be rewards received from other people (extrinsic) like a bribe or a personal sense of satisfaction (intrinsic) if an employee is looking for revenge against the organisation or possibly thinks that after the attack, he can take on the role of 'saviour' in the organisation as he has a private set of backup copies of data or some way of identifying the cyber-criminal. The possibility of selecting the maladaptive response (not to protect the system against attack) will increase due to the size of the maladaptive rewards. In contrast, increased threats will decrease the likelihood of choosing the maladaptive response (Clubb & Hinkle, 2015). The way individuals assess threat and reward differ and are not entirely predictable (Clubb & Hinkle, 2015).

Coping appraisal

Coping appraisal entails the assessment of one's capability to avoid and deal with a threatening event (Menard et al., 2017). The three factors that make up coping appraisal are response efficacy, self-efficacy, and response cost (Menard et al., 2017). The individual takes into consideration the efficacy of the recommended responses to avoid that threat (will it work) and the self-efficacy about the actions required for protection to mitigate that threat (whether they believe that they can, in fact, do what is required to avoid the threat) (Clubb & Hinkle, 2015). The third factor is what the cost will be in terms of time, effort and extra resources (Clubb & Hinkle, 2015). Further insights are that the decisions made by the person who is threatened are based on whether they can copy the behaviour of others (leading to a belief of self-efficacy).

Fear appeals (mentioned above as part of threat appraisal) also address aspects of the efficacy statement (Clubb & Hinkle, 2015; Menard et al., 2017). Fear appeals usually consist of

recommendations, and these in turn prompt people to form perceptions about two aspects of efficacy, namely, how effective the recommended response (response efficacy) will be, and about the ability of an individual to carry out the recommended response (self-efficacy) (Clubb & Hinkle, 2015; Menard et al., 2017). Two components from the coping appraisal factor were used in this study: response efficacy and self-efficacy. Therefore, PMT provides insights into to any threat to which an effective suggested solution exists that an individual believes they are able to use to defend themselves (Bigsby & Albarracin, 2022).

Justification for not using Protection Motivation Theory

The similarity between PMT and other motivation theories is that it arouses, sustains and directs how individuals should respond to threats (Clubb & Hinkle, 2015). Cyber-security relies on everyone playing their part in ensuring security (Anderson & Agarwal, 2010). PMT theory was a serious option for use in this study because it encourages people to follow through on recommended security measures - intentions result from effective persuasion (Wu, 2020). The theory predicts that users of DHIS will be encouraged to adopt the necessary security measures to protect the system from cyber-attacks and protect patient data. However, PMT was, however, *not* used in this study since it is very similar to Technology Threat Avoidance Theory that was used instead.

3.3 Theoretical foundations

The following section discusses the theoretical foundation that underpins the study. The primary purpose of the chosen theories is to help the researcher investigate how and why certain things happen the way they do. As noted above, various theories were examined to check their suitability for the study. The decision regarding the choice of underpinning theories was primarily based on the research objectives and goal. Theories selected for this study are Technology Acceptance Model (TAM), Technology, Organisation Environment Theory (TOE), and Technology Threat Avoidance (TTAT). These theories and their suitability for the study are briefly discussed below.

3.3.1 Technology, Organization, and Environment (TOE) framework

The Technology Organisation Environment framework offers contextual ways to analyse the organisational adoption² of an information system (Tornatzky et al., 1990). The three TOE constructs, namely, the environmental, technological, and organisational contexts, contain possibilities and constraints that clarify technology adoptions. These three contexts are all linked to the decision-making process for technical inventions, as shown in Figure 3.3 but the factors related to each context are not all shown in Figure 3.3.

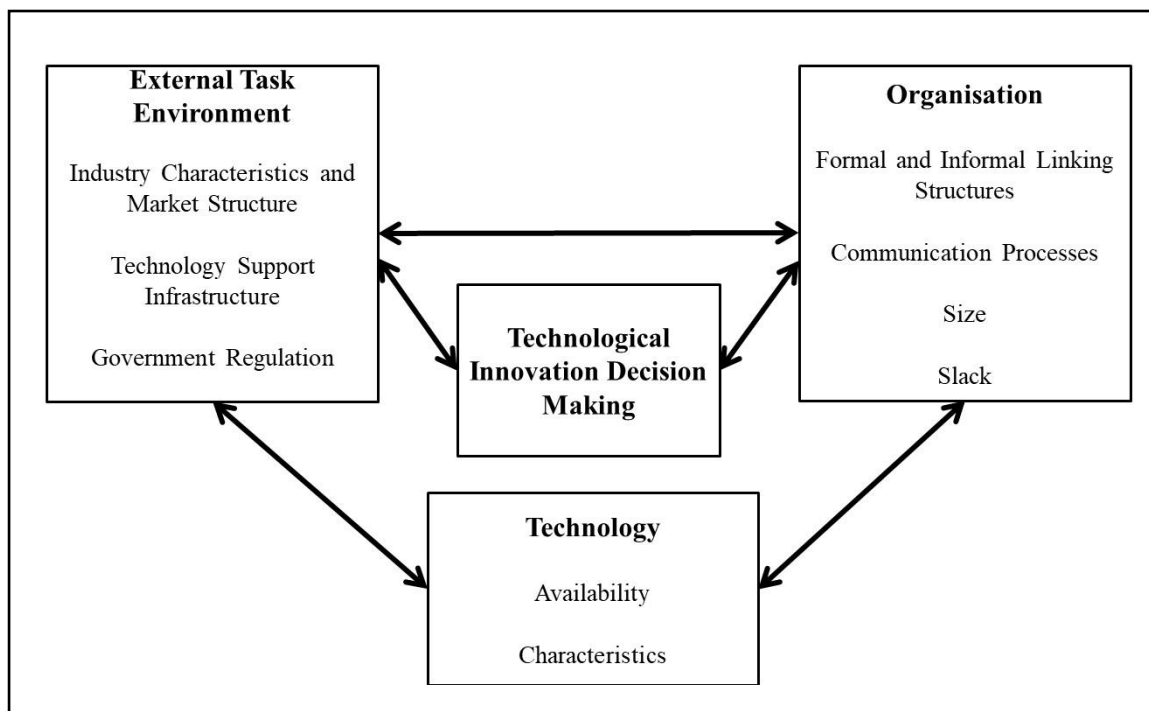


Figure 3.3: Technology-Organization-Environment Framework (Tornatzky and Fleischer, 1990)

This framework is suitable for analysing innovations in technologies related to future or existing positions with uncertainties to adopting a specific technology in the context of a working environment (organisation) (Oliveira & Martins, 2011). Two contexts were selected for this study (technological and organisational), each of which has related factors. Amongst the Technological characteristics, Training was identified as the most relevant and hence

² Note that the term organization refers to the decision taken by the decision maker to acquire the technology and to create policies and processes to allow, encourage and even require its use within the organization.

selected, and under the Organisational communication factor, the Top Management Support was considered most relevant and hence selected. The TOE framework has been widely used for information technology adoption in academic studies of various organisational types, including but not limited to Health Information Technology and E-health, E-commerce and social network sites (Larosiliere et al., 2017; Zhu & Kraemer, 2005).

Technological factors

The technological context emphasises how the functionality or features of the specific technology influence the adoption decision. Technological factors are descriptors of both external and internal technologies related to the organisation or future and current technologies (Baker, 2012). These technologies comprise equipment and associated operations available to the organisation (Baker, 2012). ICT infrastructure, security, software quality, ICT skills and hence training, user time, reliability, and perceived technology benefit are possible factors (Baker, 2012). New features can be provided by means of technological considerations to existing or new systems (Baker, 2012). For this study, the technological context was used to assess the efficacy of DHIS's cyber-security policies with a set of questions relating specifically to the perceived effectiveness of security software. This set of questions was combined with a second set focussing on the perceived effectiveness of security policies and privacy protection measures, which are not as explicitly related to technology. According to Baker (2012), the technological factors will assist the researcher in identifying whether the characteristics of the associated technology are likely to persuade users to adopt novel or enhanced methods of safeguarding the DHIS (Baker, 2012).

Organisational factors

Organisational factors include the organisation's technology readiness, culture in and around the organisation, size, communication practices and patterns, and employees' competencies. In the context of this study, 'organisational factors' refers to the characteristics of a healthcare organisation that influence a decision to adopt cyber-security controls. According to studies done by various authors such as (for example, Bhuyan & Dash, 2018; García et al., 2018; Palos-Sanchez, 2017; Senarathna et al., 2018), the size of the organisation is an essential factor that influences the rate of technology adoption. The studies show that large organisations have the resources required to use to protect themselves from the risks associated with adopting new

technologies (Bhuyan et al., 2018). On the other hand, small businesses may have insufficient means to shield themselves from the risks of adopting new technologies. However, numerous other studies suggest that the organisation's size has little bearing on the success of implementing new technology and managing risk (for example, Loukis, Arvanitis, & Kyriakou, 2017; Rahayu & Day, 2015).

Organisational factors in this study refer to managerial structure, size, organisational culture, Top Management Support, and scope. According to Ismail and Ali (2013), satisfaction or discontent with manual systems, ICT personnel knowledge, and organisational readiness influence innovation adoption. Some organisational factors promote the communication processes between top management and employees, and these include describing the purpose of innovation within the organisation's overall strategy and showing subordinates how important innovation is to the organisation. Another important organisational factor is the availability of a skilled executive team that can build a persuasive vision of the organisation's future (Ismail & Ali., 2013).

Environmental factors

Environmental factors influence the organisation's business (Al-Hujan et al., 2018). This describes how the business interacts with the government and competing industries (Oliveira & Martins, 2011). The presence lack of regulatory bodies, technology service providers, and the industry structure are all examples of environmental factors (Baker, 2012). In the case of cyber-security the presence of legislation (see Sections 2.9 in Chapter 2) fits in this category.

Justification for using the TOE framework

Oliveira and Martins (2010) found that the Technology, Organization, and Environment framework provides a solid theoretical foundation and can produce relevant results when used in studies of information system adoption. The TOE framework plays a significant role in understanding the adoption of new technologies in organisations (Wallace, Green, Johnson, Cooper & Gilstrap, 2021). The research reported on in this dissertation is located within an organisation and refers to people working within the organisation. The broader context within which the environment is located is considered to have an influence on the compliance of the workers with security controls. As discussed in Section 2.9 of Chapter 2, cyber-security

legislation exists and is very important in protecting confidential data, as is found in healthcare. This framework provides information regarding technology adoption, and authors note that there are differences between technology adoption, technology acceptance (as discussed with the Technology Acceptance Model in the next section, Section 3.3.2) and Threat Avoidance (as discussed with the Technology Threat Avoidance Theory in section, Section 3.3.3), it was chosen for this study. However, TOE is recognised to be flexible, and it is also built on sound theoretical underpinnings that are regularly validated by empirical evidence (Oliviera & Martins, 2011) believe. This framework can be adopted in different industry and social contexts because of its flexibility in contrast with other models and theories that specify different variables in each situation (Zhu & Kraemer, 2005). Thus, the TOE framework is a generalisable theory that may identify significant sources of impact without requiring the specification of new variables in each circumstance. Researchers may select different organizational, technological, and environmental elements for different studies. Two organizational and technological factors were selected from TOE for this study, namely Training and Top Management Support.

3.3.2 Technology Acceptance Model (TAM)

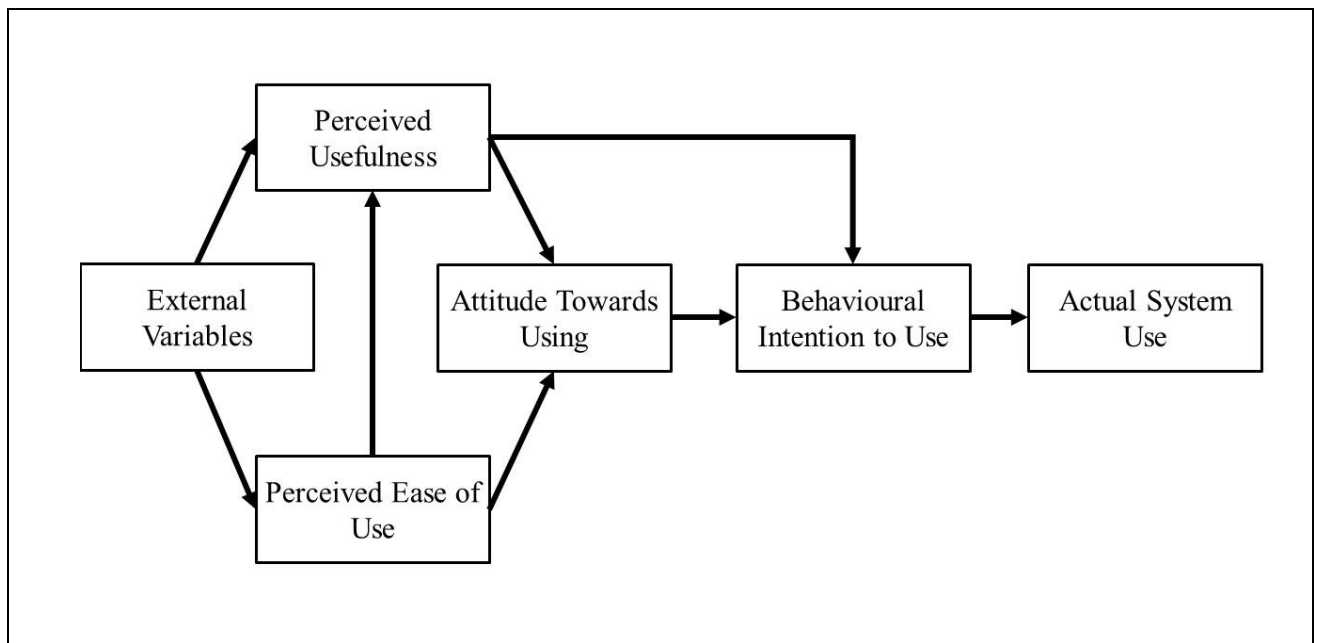


Figure 3.4: Technology Acceptance Model (Davis, 1989)

The Technology Acceptance Model (TAM) is an Information Systems theory that models how users come to accept³ and use technology (Labuschagne, Burke, Veerasamy & Eloff, 2011). TAM was introduced by Fred Davis in 1989 (see Figure 3.4) and is based on the Theory of Reasoned Action (TRA) (Nunes, Portela & Santos., 2018). It focuses on the use of the technology at the level of individual users. The TAM model illustrates the relationships between the factors influencing technology acceptance for various end-user computing technologies and groups of individual users (Labuschagne et al., 2011). Davis originally developed the TAM model to understand the process of end-user acceptance to ensure a successful implementation of an information system (Nurqamarani, Sogiarto & Nurlaeli, 2021). The TAM model indicates that users will choose to employ a new technology based on its utility and simplicity (Labuschagne et al., 2011). Furthermore, when users believe that a new technology or system will make it easy for them to perform their tasks, there is a higher probability of willingness to accept it as a useful technology (Assegaff, 2014).

The TAM model can provide a theoretical foundation for user acceptance testing, allowing system designers and implementers to assess the usability of a proposed system (Nurqamarani et al., 2021). This model is used to explain the acceptance of technology by an individual through questionnaires and subsequent analyses of them (Nunes et al., 2018). According to TAM, the user acceptance of a new system or technology is influenced by three major factors, namely, *Perceived Ease of Use* (PEOU), *Perceived Usefulness* (PU), and attitude (Nurqamarani et al., 2021). The central factor is an attitude; nonetheless, attitude is influenced by *Perceived Ease of Use* and *Perceived Usefulness*; *Perceived Ease of Use* and *Perceived Usefulness* influence attitudes towards technology, influencing the intention to use it (Nunes et al., 2018).

Justification for using Technology Acceptance Model

TAM's overall explanatory strength across various technologies, users, and organisational contexts has received a lot of empirical validation (Mahindra & Whitworth, 2005). Compared to more recent models and frameworks, TAM has a very solid theoretical foundation and

³ Note that 'acceptance' indicates that a user of the technology is employed by an organization that has already adopted the technology and requires the employee to use it. Nevertheless, within organizations employees often find ways of minimizing their use of the technology.

extensive empirical evidence and is IT-specific (Mahindra & Whitworth, 2005). Hence TAM seems to have persisted as the current dominant model for investigating technology acceptance by users, particularly amongst novice researchers. However, while TAM is appropriate for individual end users in organizational contexts and this study is undertaken at the organizational level, other frameworks may be better for individual contexts (Nurqamarani et al., 2021). The respondents who participated in the research being reported on in this dissertation are individual end users in the organizational context of Tshwane Regional Health Centres and the broader organisational context of the Gauteng Department of Health. Hence, some of the factors from TAM are appropriate to include. Factors adopted from TAM are *Perceived Ease of Use* and *Perceived Usefulness*.

3.3.3 Technology Threat Avoidance Theory (TTAT)

Technology Threat Avoidance Theory (TTAT) is a relatively recent theory (considerably more recent than TAM and TOE) that was developed by Liang and Xue (2009) for use in the context of Information Technology security. The theory was developed to explain the behaviour of individual Information Technology users when avoiding a threat (Peng & Hwang, 2021). Hence, TTAT describes how and why individual ICT users engage in threat avoidance behaviours (Liang & Xue, 2009). According to TTAT, ICT threat avoidance behaviour is a cybernetic process in which users try to close the gap between their current privacy concerns and identify potentially dangerous outcomes (Peng & Hwang, 2021). Numerous reports and articles referring to different contexts of use, such as risk analysis, healthcare, psychology, and information systems, have been used to develop TTAT theory (Carpenter, Young, Barret & McLeod, 2019). The original Liang and Xue (2009) model is shown in Figure 3.5. The TTAT framework focuses on the user level. In the ICT realm, TTAT suggests that the way that users perceive a threat will influence the way in which they will take preventive measures against it (Liang & Xue, 2009). Liang and Xue (2009) tested their theory by verifying the theoretical underpinnings of TTAT and using their model to explain technology threat avoidance behaviour.

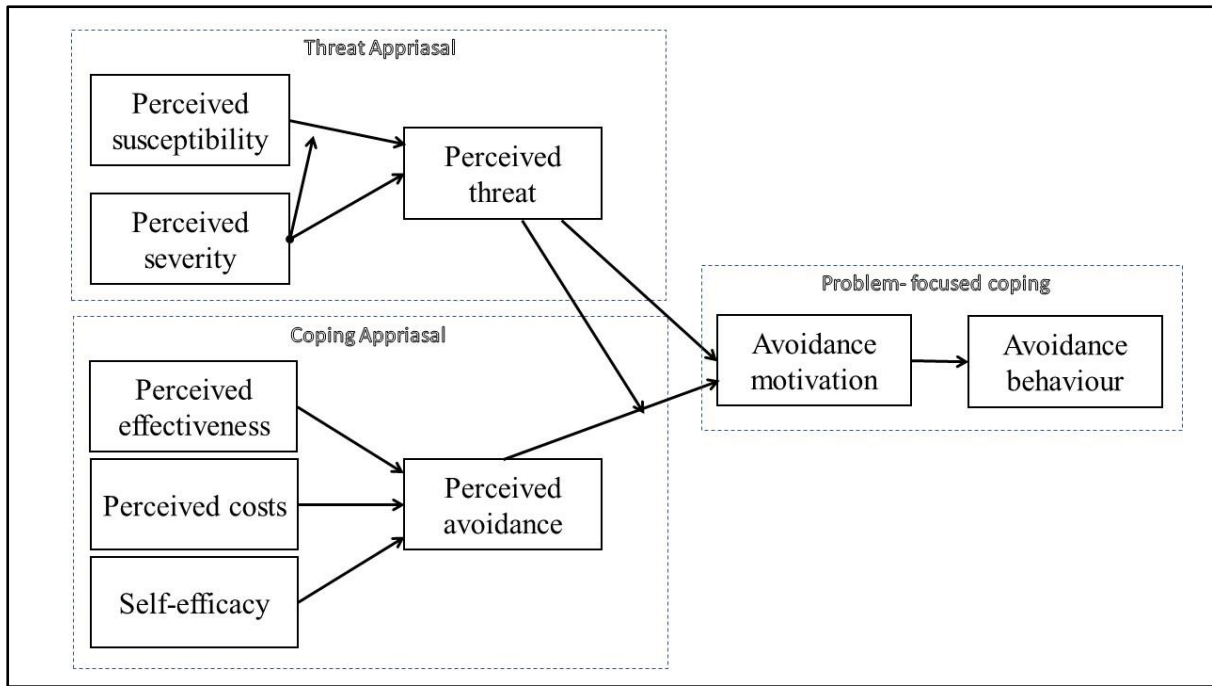


Figure 3.5: Technology Threat Avoidance Model (adapted from Khan, 2017)

TTAT is very similar to PMT, which was described in Section 3.2.4. Also, as is the case with PMT, TTAT indicates two cognitive processes users undertake when exposed to threats: threat appraisal and coping appraisal (Liang & Xue, 2009). Threat appraisal is when users assess if there is a threat and to what degree that threat will affect them. Coping appraisal is when users assess how they will avoid that threat (Liang & Xue, 2009). Thus, the essential tenet of TTAT is that users will take precautions to actively avoid an ICT threat when they believe they are exposed to it (Sylvester, 2022). Also, users will only engage in avoidance behaviour if they think taking precautions would help them avoid the hazard (Liang & Xue, 2009). As can be seen from the names of many of the factors, the data obtained from the respondents reflect perceptions rather than independently measured values. For example, *Perceived Susceptibility* is the personal assessment by an individual of the possibility of the DHIS being exposed to a threat (Wu, 2020).

An increased *Perceived Threat* (identified during Threat Appraisal) and increased *Perceived Avoidability* (identified during Coping Appraisal) increase the motivation of a user's avoid behaviour (Young, Carpenter, & McLeod, 2016). In turn, highly motivated users (*Avoidance Motivation* increases) are likely to apply threat avoidance measures (*Avoidance Behaviour*

becomes more positive) if they perceive a threat and believe that there is a safeguard measure that can help them avoid it (Young et al., 2016).

A user's conviction that harmful technology such as a cyber-attack, could have a serious negative impact on their devices, systems, business, and customers is known as *Perceived Severity* (Khan, 2017). Similar to *Perceived Severity*, *Perceived Susceptibility* is a person's opinion of the ease with which malicious technology is able to harm their equipment and systems (or how exposed to damage their systems are) (Khan, 2017). TTAT states that a user's perception of a threat (*Perceived Threat*) is influenced by the user's assessment of the chance or likelihood that the threat will materialize (*Perceived Susceptibility*) and the seriousness of the threat's adverse effects (*Perceived Severity*) (Carpenter et al., 2019).

There are three criteria that users can use when evaluating whether to make an effort to avoid a threat (*Perceived Avoidability*): These are *Perceived Cost*, *Perceived Effectiveness*, and *Self-efficacy* (Carpenter et al., 2019). Once again, these factors correspond closely with three factors that make up the coping appraisal in PMT, namely response efficacy, self-efficacy, and response cost (see Section 3.2.4), and they will not be explained again here.

TTAT also indicates that users apply *problem-focused coping* and *emotions-focused coping* techniques to assist them in deciding on threat avoidance measures when they perceive a threat (Carpenter et al., 2019)⁴. When users believe that available safeguarding measures will not help them avoid the threat, they rely on emotion-focused coping (less rational ways of coping) to prevent the threat from becoming active or try any means possible to recover (Peng & Hwang, 2021). Emotion-focused coping seeks to create a misleading belief about the environment (Chen & Laiang, 2019). Users might, for instance, ignore warnings and wish a threat would go away. As a result, without altering the actual truth, the emotion-focused coping technique lowers motivation to deal with a problem or perceived threat in an appropriate way (Chen & Liang, 2019). Another example is that users can ignore the threat and try to avoid its existence and effect on them (Chen & Liang, 2019).

⁴ Nota Bene: Only the problem-focused coping aspect of coping has been included in Figure 3.5 which has been adapted from Khan (is.theorizeit.org Accessed 05 11 2019)

On the other hand, problem-focused coping employs changing behaviour to alter the situation in a rational way using a problem-solving strategy (Chen & Liang, 2019). Problem-focused coping usually addresses the source of the threat in practical ways by implementing safeguards, such as by upgrading passwords regularly, and installing security software such as antivirus and antispyware.

Limitation of Technology Threat Avoidance Theory

A limitation of TTAT is that it proposes that coping appraisal and threat appraisal are processes that occur at the same time or shortly after one another, and this proximity in time means that they might influence one another (Chen & Liang, 2019). However, how the two forms of appraisal connect with each other and whether this is possible is unclear. According to Chen and Liang (2019), further research is necessary to validate TTAT. The literature also shows that another commonly raised limitation of TTAT is that compared with *problem-focused coping*, *emotions-focused coping* has received little attention (Jibril et al., 2020). Liang and Xue (2009) said that to avoid this limitation, it is essential to apply both appraisals, mainly how they interact. In the conceptual framework discussed in Section 3.4, only factors relating to *problem-focused coping* are included. It is for this reason that in Figure 3.5, *emotions-focused coping* has been excluded.

Justification of TTAT

TTAT was explicitly created to understand the personal motives of users when they are faced with ICT threats at work (Chen & Li, 2017). However, it has also been used by some researchers to describe users' voluntary behaviour in a non-work environment where ICT security is optional (Chen & Li, 2017). TTAT is used to study the impact on ICT users of malicious threats as well as the effects a successful attack can have (Liang & Xue, 2009). Furthermore, the theory contends that accepting safety precautions and avoiding harmful dangers are two different things (Liang & Xue, 2009).

Despite this, according to Liang and Xue (2009), TTAT assumes that technology adoption behaviour, technology acceptance and technology threat avoidance behaviour are entirely different. This awareness of the differences between the adoption and acceptance of benevolent technology and their contrasts with cyber-security explains the need for different models in

related research; adoption theories like TAM are considered by some authors to be inadequate for research into cyber-security. This is what makes TTAT an important contribution to the ICT industry. In this dissertation, aspects from three models that are considered to complement one another are used to cover the range of concerns that seem possible factors in Cyber-attack Avoidance Motivation and encouraging cyber-attack avoidance.

This theory will be helpful in this study, which will focus on Tshwane District Healthcare Centres, since it will enable the researcher to assess what information and training needs to be in place in order for users of the DHIS to be motivated to stay safe online. The influence of motivating factors on the user's attitude towards cyber-controls, and the need for that attitude to be positive in order for the change of behaviour to take place all determine the effectiveness of cyber-security controls in the DHIS. Thus, all these aspects will be investigated. The fact that this theory can assist managers and ICT executives in raising staff awareness of security concerns is an important reason why it is relevant to this study. In this study, it is essential to consider both emotions-focussed and problem-focused appraisals when applying TTAT because ICT users are believed to apply emotional thinking to avoid a threat. The theory will, therefore, help researchers to understand why users react actively and passively to ICT threats.

Six factors (*Perceived Severity, Perceived Susceptibility, Perceived Effectiveness, Self-Efficacy, Avoidance Motivation* and *Avoidance Behaviour*) from TTAT reported by Liang and Xue (2009) were used in the study. Hence, TTAT makes the most substantial contribution to the conceptual framework that is presented in the next section.

3.4 Conceptual research framework model and hypotheses

The conceptual framework is a structure that the researcher has either selected or created as a new contribution as they believe it will best explain the predicted path and outcomes of the phenomenon being investigated (Adom, D., Hussein & Agyem, 2018). It relates to practical research (both qualitative and quantitative), and illustrates concepts, which are usually derived from significant theories and published research. The conceptual framework is used to systemize and encourage the process of obtaining information and knowledge from data (Adom et al., 2018). Furthermore, the conceptual framework provides a visual guide for the researcher showing how research problems and hypotheses will be analysed (Adom et al., 2018). It also

provides a coherent way of exploring the research problems that the researcher is trying to solve (Adom et al., 2018).

The Technology Acceptance Model (TAM), Technology Threat Avoidance Theory (TTAT), and the Technology, Organization, and Environment (TOE) framework support this current study. Protection Motivation Theory is also acknowledged as TTAT built on it and has used a great deal from it. The following section will discuss the theories utilized in this study, the factors derived from each theory, the formulation of hypotheses, and the integration of selected theories to develop the conceptual framework.

Overview of the conceptual research framework

The conceptual framework for the study was developed by integrating the following theories: TOE, TAM, and TTAT. Figure 3.6 shows the ten factors that were adopted from the three selected theories. Similar factors sometimes occur in more than one existing model. Factors were carefully selected to be compatible with the study's objectives and goals. Anderson and Agarwal (2010) highlighted the importance of theory and suggested that its use provides insights that, in turn, can be used to encourage DHIS users to carry out recommended security measures to prevent cyber-attacks.

The *Perceived Usefulness* and *Perceived Ease of Use* factors were obtained from TAM. Factors were also selected from TOE, and these are *Training, and Top Management Support*, as shown in Figure 3.6. Lastly, from TTAT, *Perceived Severity, Perceived Susceptibility, Perceived Effectiveness, Self-Efficacy, Avoidance Motivation* and *Avoidance Behaviour* were found to be relevant. In line with the above summary, this conceptual model was developed as depicted (Figure 3.6) in the study.

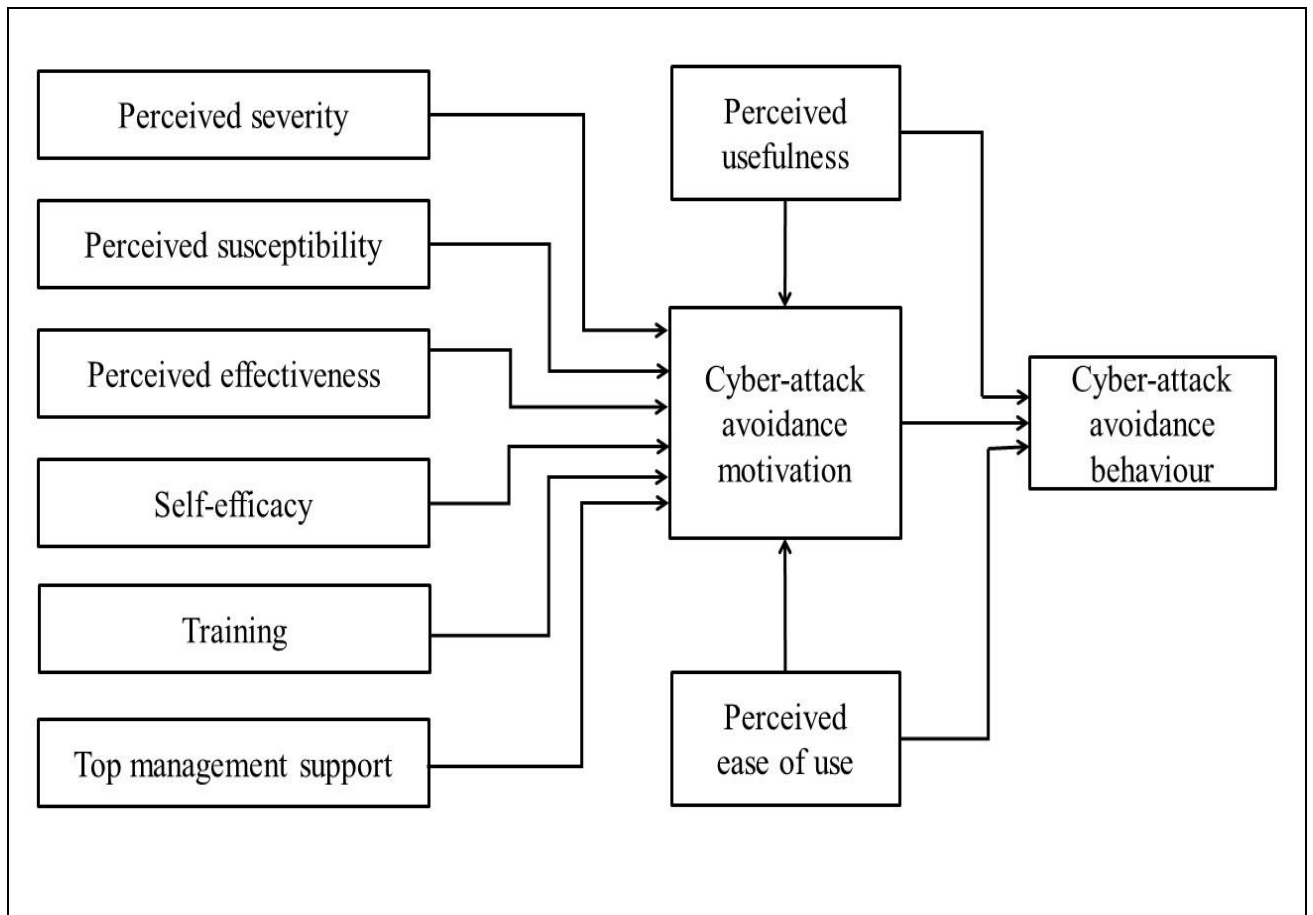


Figure 3.6: Conceptual Framework

Technology Threat Avoidance Theory

Perceived Susceptibility, Perceived Severity, Perceived Effectiveness (comprised of software effectiveness and policy effectiveness), and *Self-Efficacy* were adopted as factors from TTAT. These factors were adopted because they encourage individuals to carry out recommended security measures (*Avoidance Motivation* which also comes from TTAT). Intentions indicate effective persuasion. Hence, in the conceptual framework, *Avoidance Behaviour* is expected to be influenced by *Avoidance Motivation*. It is important to note, however, that data was not collected regarding actual behaviour change regarding cyber-attack avoidance, and hence this study does not seek to show the relationship between *Avoidance Motivation* and *Avoidance Behaviour*. As can be seen in the discussion of TAM and, in particular, Figure 3.4, *Avoidance Motivation* in the conceptual framework is similar to *Behavioural Intention to Use* from TAM

and *Avoidance Behaviour* in the conceptual framework is similar to *Actual System Use* from TAM.

Technology, Organisation, Environment framework

Technology and Organisational factors were adopted from the TOE framework to develop the conceptual framework. The *Top Management Support* factor was derived from Organizational construct, while the *Training* factor was derived from the Technological factor.

Technology Acceptance Model (TAM)

Factors adopted from TAM are *Perceived Ease of Use* and *Perceived Usefulness*.

3.5 Research hypotheses

Quantitative hypotheses reflect the assumptions a researcher makes regarding the expected outcomes of variable relationships (Creswell & Creswell, 2018). According to Creswell and Creswell (2018), the research hypothesis narrows and clearly states what the researcher wants to know (the purpose statement) and becomes a significant signpost for the reader. Once evidence (data) has been collected and analysis has been completed, the hypothesis will either be rejected or accepted. Hence, hypotheses are not conclusions; they are ideas to be tested. The conceptual framework shows the hypotheses and is given in Figure 3.6. This figure indicates the set of questions on the questionnaire used to collect data for each of the factors.

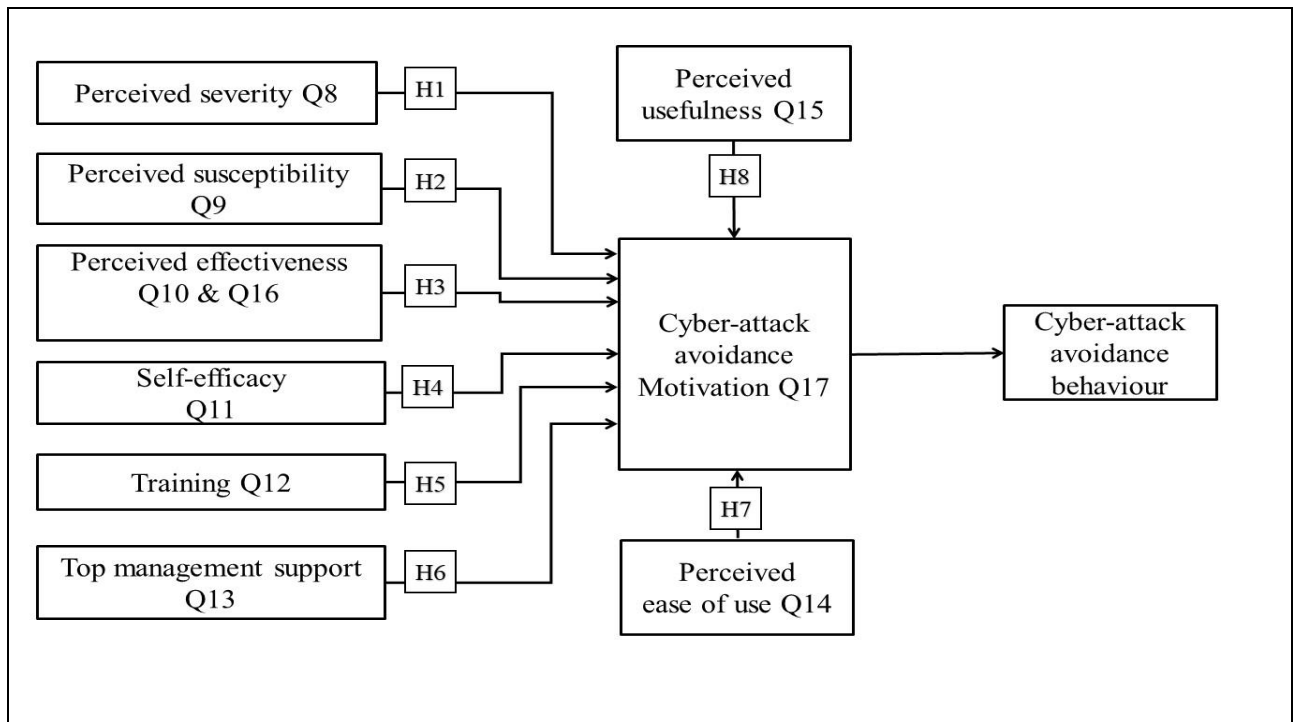


Figure 3.7: Conceptual Framework Including Hypotheses

Perceived Severity factor

To protect the DHIS, specific behaviours are used to remove or lessen the *Perceived Threat* (Van Bavel, Rodríguez-Priego & José Vila, 2019). When users perceive the severity of cyber-attacks on DHIS as being high, they are more likely to implement measures to safeguard the system (Van Bavel et al., 2019). In the context of this study, the *Perceived Severity* is the negative impact of cyber-attacks on DHIS. Suppose there is no access to medical records owing to system unavailability caused by cyber-attacks. Loss of patient data, changing medical records due to unauthorised access to the DHIS system, ransomware attacks, and loss of life due to inaccurate diagnostics are all possible implications for DHIS. It is reasonable that the respondents for this research will consider this to be a severe impact, but this is not assumed. If recommended methods to defend the system are not followed, DHIS would be vulnerable to viruses, malware, and ransomware. Hence, ultimately respondents will change their behaviour and comply with cyber-security controls and hence will contribute towards safeguarding the effectiveness of the DHIS. In other words, if the respondents *are* motivated by a perception that there will be a severe impact (perceived severity) if there is a cyber-attack on the DHIS will be encouraged to avoid cyber-attacks (Cyber-attack Avoidance Motivation).

In view of the above argument, the following hypothesis is proposed.

H1: Increased *Perceived Severity* has an increased positive impact on Cyber-attack Avoidance Motivation.

Perceived Susceptibility factor

The degree to which an individual or organisation is seen as being likely to be unprotected from threats is measured by *Perceived Susceptibility*. Unauthorised access to DHIS is defined as a threat in the context of this study. Users who believe they are indeed significantly vulnerable as a link in the system to expose the DHIS to cyber-attacks and cyber-threats will be more inclined to take appropriate actions to protect the DHIS (Wu, 2020).

In view of the above argument, the following hypothesis is proposed.

H2: Increased *Perceived Susceptibility* has an increased positive impact on Cyber-attack Avoidance Motivation.

Perceived Effectiveness factor

According to Protection Motivation Theory, when *Response Efficacy* is considered at a moderate to a high level, it leads to positive threat mitigation whereby a recommended response is acted on (Rogers, 1975). In TTAT, *Response Efficacy* is known as *Perceived Effectiveness*. If users believe that the recommended security measures are highly effective, they will be motivated to ensure they are implemented. In this study, confidence in the security department guidelines should motivate DHIS users to follow security policies set out to protect the DHIS from cyber-attacks. In the questionnaire, there were two separate sets of questions that related to perceived effectiveness (see Figure 3.7). The items in Question 10 relate to whether adherence to information security policies and protection measures (that is, controls) is an effective way of protecting the DHIS. The items in Question 16 relate to whether the use of security software is an effective way of protecting the DHIS. The data analysis described in Chapter 5 is done for the two questions separately and also takes them as a single set of data.

Users can also protect confidential information on the DHIS by effectively using information security technologies. In view of this, the following hypothesis is proposed.

H3: Increased *Perceived Effectiveness* has an increased positive impact on Cyber-attack Avoidance Motivation.

Self-Efficacy factor

When confronted with a threat, self-efficacy has a robust effect on an individual's intention to implement protective measures when faced with a threat (Tsai et al., 2022). In this study, self-efficacy relates to DHIS users' capability to set out security measures on the system to prevent cyber-attacks. It also includes the ability of an individual to use security measures such as antivirus to protect the DHIS system. Furthermore, the DHIS system is effectively protected by users' cyber-security knowledge and understanding.

In view of the above argument, the following hypothesis is proposed.

H4: Increased *Self-Efficacy* has an increased positive impact on Cyber-attack Avoidance Motivation.

Training factor

The *Training* factor was included because users will benefit from technological factors during *Training* on a new or better security software solution. This security software solution can be used to prevent cyber-attacks on DHIS. Users can be trained on installing antiviruses and be knowledgeable on cyber-attack avoidance. According to the TOE framework, the factors within the Technology construct indicate the organisation's readiness to adopt new technologies (Wallace et al., 2021). Personnel who influence decision-making on technology adoption, ICT infrastructure, and ICT software are examples of technological factors (Wallace et al., 2021). Technology adoption further influences whether the organisation is ready to adopt the technologies relevant to its business needs and available to them (Wallace et al., 2021).

In view of the above argument, the following hypothesis is proposed.

H5: Increased levels of *Training* has an increased positive impact on Cyber-attack Avoidance Motivation.

Top Management Support factor

The *Top Management Support* factor was chosen for this study because it investigates the structures relating to top management, their commitment to the infrastructural requirements and communication between employees (Kim & Kim, 2021). According to Kim and Kim (2021), it adds to the richness and multifaceted nature of the context provided by TOE and of technology use within the organisation. This will assist the researcher in determining which cyber-security motivational features are provided by DHIS. Furthermore, organisational characteristics aid in assessing the condition of cyber-security investment by top management. *Top Management Support* reveals preparedness to improve and invest in the DHIS security areas, such as user training in cyber-security, controls and processes, development of effective security policies, and security culture.

In view of the above argument, the following hypothesis is proposed.

H6. Increased *Top Management Support* has an increased positive impact on Cyber-attack Avoidance Motivation.

Perceived Ease of Use factor

In the context of this study, *Perceived Ease of Use* reflects the view of the respondents on whether existing security measures to prevent cyber-attacks are easy to use. As a result, it will influence the acceptance rather than resistance of security measures to avoid DHIS cyber-attacks (Malatji et al., 2020). In view of the above argument, the following two hypotheses were proposed.

H7: Increased levels of *Perceived Ease of Use* has an increased positive impact on Cyber-attack Avoidance Motivation.

Perceived Usefulness

Perceived Usefulness will also motivate DHIS users to keep track of any updated security measures. As a result, *Perceived Usefulness* impacts behavioural intentions when it comes to employing the DHS's cyber-security controls to prevent cyber-attacks.

In view of the above argument, the following hypothesis is proposed.

H8: Increased levels of *Perceived Usefulness* has an increased positive impact on Cyber-attack Avoidance Motivation.

Cyber-attack Avoidance Motivation

This factor was chosen for this study because it describes the attitude of users that is assumed to be necessary for avoiding threats of malicious information by an individual user using safeguarding measures available to them (Liang & Xue, 2009). In this study, the *Cyber-attack Avoidance Motivation* factor will be helpful to determine if users accept the avoidance measures, including installed cyber-security controls that are available to them. As noted in Section 3.4.2, *Cyber-attack Avoidance Motivation* is similar to *Behavioural Intention to Use* from TAM, and *Cyber-attack Avoidance Behaviour* in the conceptual framework is similar to *Actual System Use* from TAM.

Cyber-attack Avoidance Behaviour

In view of the above argument, the following relationship is proposed in the conceptual framework, but there is no hypothesis for it as evidence of actual cyber-attack avoidance behaviour (data) was not collected.

3.6 Conclusion

As explained in Chapter 1, the study's overall goal was to improve the efficacy of District Health Information System (DHIS) cyber-security controls. The researcher achieved this by examining how healthcare support staff from the Tshwane District Healthcare Centres interacting directly with the DHIS react to ICT threats. This chapter looked at several theories to determine which were most suited to the study regarding promoting cyber-security in health information systems in a group of centres making up the Tshwane District Healthcare Centres. The limitations of the theories and the justifications for the decisions to use each of the related theories were also discussed.

The theories selected differ in their goals. TOE seeks to highlight underlying factors relating to technology adoption behaviour and looks particularly at decisions made regarding the acquisition of technology and setting policies and procedures for its use. On the other hand,

TAM looks at technology acceptance – what influences the users of technology (usually software but may be software and devices) provided to them to follow policies and procedures for its use. According to Liang and Xue (2009), TTAT says that Technology threat avoidance behaviour is entirely different from adoption and acceptance of technology as it involves the adoption and acceptance of cyber-security controls that do not improve the performance of the users' main function but minimise the risk of catastrophic loss of access to essential parts of the system.

This chapter proposes that awareness of the differences between the adoption and acceptance of benevolent technology and their contrasts with cyber-security explains the need for different models in related research. In this dissertation, aspects from three models that are considered to complement one another are used to cover the range of concerns that seem possible factors in Cyber-attack Avoidance Motivation and encouraging cyber-attack avoidance.

The underpinning theories TAM, TOE, and TTAT were adopted to develop this study's conceptual framework. The eight hypotheses discussed in this chapter all investigate factors that may motivate users of DHIS to follow cyber-security control measures (Cyber-attack Avoidance Motivation). *Perceived Susceptibility*, *Perceived Severity*, *Perceived Effectiveness* (comprised of software effectiveness and policy effectiveness), *Self-Efficacy*, *Avoidance Motivation* and *Avoidance Behaviour* were adopted as factors from TTAT. *Perceived Ease of Use* and *Perceived Usefulness* were adopted as factors from TAM. *Top Management Support* and *Training* were adopted as factors from TOE.

The next chapter will discuss the study's methodology, providing details on how the study will be conducted.

CHAPTER 4: RESEARCH DESIGN AND METHODOLOGY

4.1 Introduction

The previous chapter discussed the theoretical foundation that underpins the study and the conceptual framework. Chapter 4 presents the research design and methodology which was followed in this study. In the next section, the researcher discussed the research design, philosophies as well as the research approach, the research population, sampling techniques and sample size. Data collection, analysis and interpretation, together with ethical considerations and research limitations, will also be discussed.

4.2 Research design

According to Ranjit (2019), a research design is a procedural plan the researcher decides to follow to answer research questions adequately, precisely, objectively, and efficiently. The procedural plans are translated from broad assumptions to precise step-by-step methods and strategies (Saunders et al., 2019). The researcher should make various decisions to solve the research problem and propose how they will conduct their study (Saunders et al., 2019). Methods regarding how participants will answer research questions or how the researcher will test the hypothesis are indicated in the design (Wahyuni, 2012). When the study is conducted, researchers usually set goals of what they hope to achieve (Webb & Auriacombe, 2006). Therefore, the research design is a guideline and includes instructions for reaching the study's goal (Wahyuni, 2012). Guidance on how the entire research will be conducted is articulated in the procedural plans (Saunders et al., 2019). This process helps set up how the research study intends to solve the problem (Wahyuni, 2012). Consequently, these plans present the options and, eventually, those chosen of the many choices that need to be made (Wahyuni, 2012).

Research methodologies, strategies, and philosophical perspectives are all part of designing a study (Saunders et al., 2019). The researcher's worldview should guide the selection of the research design (Creswell & Creswell, 2018). These choices are also influenced by the issue at hand (research problem), the target audience, and the researcher's own experiences (Saunders et al., 2019). The research design also addresses issues regarding the data required to answer research questions and the appropriate methods to gather data (Saunders et al., 2019). The

overall approach of the study, in particular the methodologies, is outlined under the study's purpose (Creswell & Creswell, 2018).

According to Saunders et al. (2019), the research design focuses on transforming a research problem into a research project. The design outlines the achievable plan that the researcher will use to move from the initial point (that is, the statement of the research questions that the researcher will answer) to the final point (that is, findings or outcomes of the research) (Webb & Auriacombe, 2006). These include choosing the research methodology, research strategy, data collection tools, population, and sampling procedures (Webb & Auriacombe, 2006). The following section outlines the research design the study followed to solve the identified problem: the protection of DHIS at the Tshwane District Healthcare Centres from cyber-attacks and cyber-threats.

This study used a quantitative research methodology. Furthermore, the researcher will need input from a broad spectrum of system users. There is just one truth or reality in the researcher's positivist viewpoint. This created the researcher's independence from the findings due to the objectivity of the investigation. A positivist worldview is what the researcher holds and believes only one truth or reality exists. As a result, the researcher was independent of the study because it was objective. The population of the study was Tshwane District Healthcare Centre employees with access to the DHIS. It included data capturers, Information clerks, IT Administrators, the Heads of the Departments, Facility Information Officers, Facility Information Managers, and District Information Managers. The staff at the healthcare centres who provide medical services at the Tshwane District Healthcare Centres do not generally interact directly with the DHIS. Non-probability sampling was drawn from this population using convenient and purposeful sampling techniques. Data was collected using a questionnaire as an instrument and was analysed using a statistical tool. The data collection method was suitable as it allowed easy access to participants, considering that the study population is employees in the healthcare centres who work with people's lives (Saunders et al., 2019). Finally, deductive methods were followed to collect, analyse and interpret quantitative data to make conclusions.

4.2.1 Types of research design

The purpose of research is to explore, describe or explain the research problem (Saunders et al., 2019). Some research studies are descriptive and exploratory, meaning they have more than one purpose (Saunders et al., 2019). The following section describes different research designs. Classification depends on the purpose of the research since each design serves a different purpose and end goal.

4.2.1.1 Exploratory studies

Exploratory research aims to develop new insights about a study by exploring its characteristics (Webb & Auriacombe, 2006). The researcher conducts an exploratory study to investigate or probe a new point of view or idea or to assess a phenomenon based on a research investigation where the problem is not clearly defined (Webb & Auriacombe, 2006). Therefore, this type of study is useful when the researcher wants to clarify the research problem. It investigates the problem in depth to get a more complete understanding but does not offer a conclusive solution (Saunders et al., 2019). Exploratory research begins with general ideas, and these ideas reveal issues that can be used for future research. According to Saunders et al. (2019), the primary way of conducting exploratory research is by using qualitative methods through literature research, interviews, and focus groups.

The fundamental benefit of exploratory analysis is its adaptability to new ideas because the methodology is subjective (Saunders et al., 2019). New information is revealed while the researcher does their investigation, and new facts drive this transformation (Saunders et al., 2019). A complete collection of pertinent aspects is provided by exploratory research, which enables the researcher to fully describe the reality of the situation as it currently exists (Webb & Auriacombe, 2006). An exploratory research design involves the researcher being interpretative and addressing why, what, and how questions to address the study problem (Webb & Auriacombe, 2006). Furthermore, interpreting qualitative data is subjective and is frequently biased (Saunders et al., 2019).

4.2.1.2 Explanatory studies

The primary purpose of positivist explanatory research is to explain why phenomena occur and predict if they can happen again in the future. This is achieved by studying a research problem or situation and defining relationships between variables. Causal relationships among variables are explained, and future occurrences are predicted (Webb & Auriacombe, 2006).

An explanatory study is suitable for the quantitative approach and answers questions about the how and why of a research object (Saunders et al., 2019). This is achieved by determining the correlations, causes and effects between research variables by testing hypotheses and providing profound knowledge. Explanatory research is characterised by research hypotheses that specify the direction and nature of the relationships among or between variables being studied (Webb & Auriacombe, 2006). These studies then test and validate the relationships from the hypotheses (Webb & Auriacombe, 2006). Upon conducting explanatory research, the researcher understands and sometimes predicts the consequences and intentions behind specific actions (Saunders et al., 2019). Explanatory research was appropriate for this study because it does not draw conclusions but instead focuses on the root of the issue (Saunders et al., 2019). Another issue is that the explanatory method requires the researcher to explain the phenomenon, but this study is not set up in that way (Saunders et al., 2019).

Explanatory studies also occur in interpretivist research, particularly as case studies as described in Sections 4.3.2, 4.6.2 and 4.7.1.

4.2.1.3 Descriptive study

A descriptive study aims to describe situations or events by observing and understanding specific characteristics of the phenomenon or population under investigation (Webb & Auriacombe, 2006). This is achieved by describing the nature of the study, what exists, and its frequency and categorising the results accordingly (McGregor, 2019). Questions about what, how, and when are answered in the descriptive study. The researcher, therefore, attempts to describe what they know about the phenomenon based on their observation (Webb & Auriacombe, 2006). However, this method does not tell us why a particular event happened in a certain way or the reasons behind specific actions (Webb & Auriacombe, 2006). The data collected from a descriptive study can be either quantitative or qualitative (Saunders et al.,

2019). Research under a descriptive survey is objective, and the results are conclusive. The conclusions drawn can be generalised from the sample to the population (McGregor, 2019).

A survey was followed in this study. This research examines ways to improve the effectiveness of cyber-security controls in South African public healthcare centres to prevent cyber-attacks focusing on Tshwane District Healthcare Centres. Shuttleworth (2008) argues that descriptive research design is a scientific method that includes observing and portraying a subject's conduct without impacting it in any way (Webb & Auriacombe, 2006). Factors of human behaviour that contribute to the effectiveness of cyber-security controls in DHIS are described in this study. Descriptive study helped the researcher understand the behaviour of humans in a way that exposes the DHIS to cyber-threats and how cyber-security controls can be implemented effectively to protect the DHIS. Another important factor regarding the descriptive approach was that the research did not manipulate or influence results. The researcher did not know much about the cyber-security controls in DHIS and therefore collected relevant data to address the research problem.

4.3 Research Philosophy

Research philosophy is defined by (Saunders et al., 2019) as the assumptions and beliefs about knowledge development. When researchers embark on their study journey, they use philosophical views to help them develop knowledge in a specific field of study (Saunders et al., 2019). According to Hammersley (2004), philosophical assumptions are based on how one views the world to strengthen the research methods to be followed when conducting research (Hammersley, 2004). It is a belief in how data about a phenomenon should be collected, used, and analysed (Hammersley, 2004). The beliefs guide the researcher's action and thus influence the nature of research and the researcher's choices about a particular field of study (Creswell & Creswell, 2018).

Kivunja and Kuyini (2017), in their paper, stated that a worldview is the set of beliefs, perceptions, ideas, school of thought, or thinking that articulates the interpretation and meaning of research data. Philosophy implicitly denotes the researcher's worldview. It expresses the conceptual ideas and convictions that shape the researcher's worldview, behaviour, and interpretation of their surroundings (Kivunja & Kuyini, 2017). According to Saunders et al.

(2019), how you perceive the world shows how you perceive it to be and what you perceive it to be there for. Furthermore, it determines the procedures for gathering and analysing data (Kivunja & Kuyini, 2017). The four main philosophical schools are covered in the section that follows (positivism, interpretivism, pragmatism, and realism). Similarly, the rationale for the chosen philosophical perspective that served as the study's direction will also be discussed.

4.3.1 Positivism

The positivist philosophical view states that some ("positive") knowledge is grounded on normal phenomena, their relations, and properties (Martyn, 2004). According to Creswell and Plano (2011), positivism believes that reality is constant and can be perceived and defined objectively. This means that a single truth or reality needs to be understood, discovered and measured quantitatively. The data used in this type of research is from empirical evidence; thus, in this case, research should be observed directly using the human senses (direct observation and measurement) (Martyn, 2004). This philosophy is suitable for analysis using quantitative statistical research methods and is highly structured, allowing the outcome to be generalised (Martyn, 2004). Objects can be measured, analysed, and evaluated using statistical tools, and the outcomes are objective, dependable, and consistent and thus represent reality (Creswell & Plano, 2011). Since positivist researchers are thought to be objective, they are neither affected by nor prone to subjective influences (Creswell & Plano, 2011). However, according to Saunders et al. (2019), simplifying observations from the real world into laws and generalizations may result in a shallow understanding of reality that hides complexity. Nevertheless, one could contend that data collected through surveys provide reliable and precise measurements in the context of cyber-security policies in healthcare facilities. Therefore, the positivist philosophy using the quantitative technique was applied in order to derive trustworthy and legitimate conclusions.

Justification for the use of the positivist philosophy

This study, as has already been said, adopted a positivist philosophical approach. The choice is justified by the researcher's intention to evaluate the effectiveness of DHIS's cyber-security measures. In addition, this was done by collecting quantitative data from the participants, analysing the data, and drawing conclusions using statistical techniques. This mindset made it

possible to establish a connection between DHIS users and efficient countermeasures against cyber-threats. In addition, the approach measured and quantified the observable to transform it into an outcome that allowed for scientific verification. Quantitative research paved the way for additional research.

Furthermore, the positivist approach assisted in developing hypotheses that were tested to evaluate the relationships between variables. The research was objective, and the results of the hypotheses could be generalised in a larger context that uses DHIS systems. Since positivism adopts an objective methodology, the researcher had no influence over the results of the study. Additionally, it enabled the involvement of a large number of participants, which helped the researcher attain a satisfactory sample size as needed for statistical analyses.

4.3.2 Interpretivism

Interpretivism is also known as Constructivism or social Constructivism (Saunders et al., 2019). According to Saunders et al. (2019), reality is believed to be socially constructed, with ongoing interaction between the researcher and what the researcher is observing and is constrained by any limitations the researcher might face. Interpretivism is suitable mainly for qualitative research (Creswell & Plano, 2011). Scientists using the interpretivism paradigm set out to understand, explain, and clarify social reality using what is said by different participants regarding how they view the context of the research (Creswell & Creswell, 2018). Meanings of human behaviour are interpreted instead of trying to identify generalised and predicted causes and effects.

Different individuals' personal experiences form their world's views, and the interpretivism paradigm focuses on understanding the world (Louis et al., 2007). Furthermore, interpretivism seeks to find meanings by using tools like interviews or observing participants directly. The interpretivist philosophy was not suitable for this study mainly because the researcher is by nature objective and therefore seeks a large number of participants contributing data and results that can be generalised in similar contexts but different geographic locations.

4.3.3 Realism

Realism concurs with the idea that things are not always as they seem and that entities may thus have objective realities that may be different from how people perceive them to be (Louis et al., 2007). Realists assert that everything in the universe serves an objective purpose (Lincoln & Guba, 1995). According to realists, everything in the universe serves some sort of objective purpose (Lincoln & Guba, 1995). However, the objective interpretation of the purpose by the role-players interacting with it may be different from the actual purpose. Additionally, it emphasizes the necessity of putting to the test subjective interpretations in order to arrive at specific objective meanings. For this study, realist philosophy was deemed unsuitable.

4.4 Research paradigms

Researchers make various assumptions in their research, either consciously or unconsciously (Saunders et al., 2019). Research paradigms are composed of three fundamental components: ontological, epistemological, and axiological assumptions (Saunders et al., 2019). Every paradigm has underlying presuppositions, convictions, standards, and ideals. As a result, the chosen paradigm's presumptions, values, and beliefs serve as a guide and a limiting factor for the research investigation (Kivunja & Kuyini, 2017). Therefore, philosophical assumptions automatically influence how researchers understand the research topic, the research methods used, and how the findings should be interpreted (Saunders et al., 2019). Three major paradigms are discussed in the following section, which are: epistemology, ontology, and axiology and clarifies the paradigm used in the study and justification thereof (Saunders et al., 2019).

4.4.1 Ontology

Ontology is defined by Rehman and Alharthi (2016) as "the nature of our beliefs about reality." It is about making assumptions as a way to reach a belief that something is genuine or makes sense (Kivunja & Kuyini, 2017). Researchers have assumptions about reality that they unconsciously depend on when they understand things; these are their basic assumptions about whether reality exists, and what is known about it (Martyn, 2004). Therefore, researchers use ontological questions to enquire about the kind of reality that exists in their study (Rehman &

Alharthi, 2016). Saunders et al. (2019) claim that ontology has an impact on inquiries into a researcher's presumptions about how the world functions and the reason why one has a specific view. It concerns our worldviews, or how we perceive the world, and as a result, our beliefs, or what is sincere and makes sense to us (Rehman & Alharthi, 2016).

Reality concepts about what the researcher believes can be known from that reality and can be formulated using the ontology paradigm (Rehman & Alharthi, 2016). Furthermore, it examines the researcher's fundamental belief about nature's existence (Kivunja & Kuyini, 2017). The nature of reality assumptions is essential because they assist the researcher in understanding how to make meaningful conclusions from the collected data (Martyn, 2004). This ontological assumption helps position the researcher's thinking about the problem they are trying to solve, the significance of the study, and how the researcher will solve the problem (Kivunja & Kuyini, 2017). According to Kivunja and Kuyini (2017), a researcher could inquire about the existence of reality when making ontological assumptions. Do one's thoughts construct or create reality? What kind of thing is reality? So, is reality subjective or objective? Does each person's experience determine reality? The significance of the study, research challenges, and prospective study techniques are thereby positioned in the researcher's mind using ontological assumption notions (Kivunja & Kuyini, 2017). Furthermore, these hypotheses can help in comprehending and resolving the problem being investigated (Kivunja & Kuyini, 2017)

4.4.2 Epistemology

Epistemology is defined by Rehman and Alharthi (2016) as the study of the nature of knowledge and justification. They further explain that this philosophy articulates the processes of acquiring and validating knowledge (Rehman & Alharthi, 2016). According to Du Plooy-Cilliers Davis and Bezuidenhout (2014), epistemology is interested in how knowledge develops naturally, how to advance it, and how to communicate it with others. The term "acceptable knowledge" about a particular study is defined by epistemology (Du Plooy-Cilliers et al., 2014). It also has to do with the kind of knowledge and comprehension the researcher or knower can pick up. Epistemology aids in the growth, extension, or enlargement of deeper research knowledge (Kivunja & Kuyini, 2017). According to Saunders et al (2019), Epistemology refers to the theory of knowledge, how we know what we know. It illustrates how we ended up knowing what we know and how we know reality or the truth (Saunders et

al., 2019). According to Kivunja and Kuyini, (2017), the questions researchers might ask when thinking about epistemological presumptions include Is knowledge acquired on the one hand, or is it based on one's personal experience? (Kivunja & Kuyini, 2017). What is the connection between what should be known, the knower, and the nature of knowledge? What connection exists between the asker and the information that is already known? These types of inquiries are essential to the epistemological premises because they assist the researcher in establishing the context for their research (Kivunja & Kuyini, 2017). Given what is already known, the epistemology questions aid researchers in learning what new knowledge or new insights is (Saunders et al., 2019).

The vital question on the epistemological element paradigm that researchers should understand is "How do we know what we know?". This question is based on investigations of the truth (Kivunja & Kuyini, 2017). However, there might be debates about such a thing as 'truth' and what counts as 'truth?' And what we consider as 'truth,' and if we believe factual evidence as 'truth' (Du Plooy-Cilliers et al., 2014). Epistemological assumptions help researchers ask factual questions like how one knows this is the truth. (Du Plooy-Cilliers et al., 2014). Correspondingly, it aids in the researcher's discovery of novel ideas related to their research, as well as of what is already known and what counts as knowledge. Furthermore, according to Kivunja and Kuyini (2017), what constitutes legitimate, acceptable, and valid knowledge? This premise will determine how much the researcher adds to the body of knowledge as a result of the study (Saunders et al., 2019).

4.4.3 Axiology

McGregor (2019) defines axiology as the values and ethics of the research study. Axiology includes questions about how researchers deal with their values and the values of those who will participate in the research study (Du Plooy-Cilliers et al., 2014). This philosophical assumption determines our values' role in our research choices (Du Plooy-Cilliers et al., 2014). It is an ethical consideration when conducting research (McGregor, 2019). Axiological assumptions study values judgment (Saunders et al., 2019). It is concerned with social inquiries. The role played by the researcher's values in all phases of the study is essential as it leads to credible research results (McGregor, 2019).

Humans are governed by their values, say Kivunja & Kuyini (2017), which inform their behaviour. Axiological abilities show a researcher's capacity to communicate their beliefs based on choices regarding the research they have undertaken (Saunders et al., 2019). The decisions made by the researcher in their study reflect their values (Du Plooy-Cilliers et al., 2014). There are options for the philosophical perspective, the study's subject as opposed to others, data gathering techniques, and analytics (Saunders et al., 2019). Axiological presumptions aid the researcher in comprehending, defining, and assessing the correct and incorrect notions pertinent to the investigation (McGregor, 2019). It reflects the values that should be attributed to various aspects of the study, the people we are researching, and the data and people we shall report the study's findings (Kivunja & Kuyini, 2017). According to Saunders et al (2019), the question as to what the nature of ethical behaviour or ethics is, is answered by axiological assumptions. When answering this question, researchers must consider what they regard as the human values of everyone participating in the research study (Kivunja & Kuyini, 2017). Axiology takes into account issues like the values that the researcher follows when carrying out a study. What actions should be taken by the researcher to uphold the rights of each participant? What traits and values ought the researcher to possess? Will the study be carried out respectfully and without conflict? How can risk be reduced? 2019 (Saunders et al.). Researcher's values influence how the entire study will be conducted and are taken into account in the research findings, and these axiological assumption questions are crucial (McGregor, 2019).

4.5 Objectivism and subjectivism Philosophical assumptions

Objectivism is consistent with natural science assumptions (Saunders et al., 2019). It argues that just like in the natural sciences, social realities exist independently and externally to us (Creswell & Creswell, 2018). Saunders et al. (2019) agree with this view; objectivism embraces realism and asserts that social entities are of the natural world and exist independently of social actors. According to this view, the existence of social entities is not influenced by the experience and interpretation of social actors. Therefore, objectivist assumptions believe that all social actors experience only one actual social reality (Creswell & Creswell, 2018). Consequently, objectivism pursues uncovering the 'truth' about the social world. This truth is uncovered by observing facts that can be measured from generalised laws derived from

universal social reality (Creswell & Creswell, 2018). Objectivist researchers try to keep their research free of value judgements that bias their conclusions (Saunders et al., 2019). Furthermore, they strive to prevent their own beliefs and values from clouding their analysis and findings throughout the research study (Saunders et al., 2019)

On the other hand, subjectivism includes assumptions commonly encountered in academic studies in the humanities and arts (Creswell & Creswell, 2018). It affirms that social phenomena are made up from the actions, languages, and perceptions of concerned social actors and are embedded in their existence (Saunders et al., 2019). According to Creswell and Creswell (2018), subjectivism states that all aspects of the accomplishments of social actors are shaped through their meaning and social phenomena. Subjectivism is an epistemological position that focuses on how social actors interpret events, tell stories, and perceive and express social realities (Saunders et al., 2019). This is based on an underlying view e that the social world has no essential existence other than what individuals attribute to it. Because each person perceives reality differently and has a unique experience, subjectivism embraces and expresses many realities as opposed to a single reality that applies to everyone (Saunders et al., 2019).

Justification of choice

This study follows an assumption that reality is objective. This is because the researcher accepts that the social entities on the effectiveness of cyber-security control in DHIS are external to her. Another reason is that objectivism allows the researcher to collect factual data which can be described, measured, and observed quantitatively (Creswell & Creswell, 2018). Hence questionnaires were administered to DHIS users in selected healthcare centres.

4.6 Research approach

The approach outlines the methods and procedures used by the researcher to identify the steps needed to understand a particular phenomenon and to address a research issue (Creswell & Creswell, 2018). Depending on what data is considered to be relevant and the accessibility of the data to be collected, different approaches can be taken. Researchers choose an approach based on the subject, research problem, population, and personal experience. In order to confirm hypotheses and theories, research methodologies exist that are described as being

qualitative, quantitative, or mixed. The development of each of these methodologies has been influenced by various strategies, designs, worldviews, and methods (Wahyuni, 2012).

The study followed a quantitative approach, which allowed the researcher to collect numerical data and statistical analysis. The following section discusses the commonly used research approaches for data collection, which are quantitative, qualitative and mixed methods. Furthermore, the justification for the chosen approach was also discussed in this section.

4.6.1 Quantitative research approach

According to Creswell and Creswell (2018), a quantitative research approach achieves the given research objectives by exploring relationships between variables (Creswell & Creswell, 2018; Myers, 2013). These variables are names for subcollections of numeric data obtained from measurements, usually by means of instruments (including questionnaires); analysis is done on numbered data use statistical procedures (Creswell & Creswell, 2018). Collected data measures reality objectively to discover its meaning. The quantitative approach uses numbers obtained from closed-ended questions in an online, telephonic or paper-based survey. It may alternatively use automated data collection, such as from technological devices and quantitative experiments (Myers, 2013). Furthermore, its approach is of a positivist worldview which believes that one truth or reality needs to be understood and uncovered (Saunders et al., 2019). Quantitative research is generally associated with a set of objective assumptions and with positivism.

Advantages of quantitative research

The primary benefit of the quantitative research paradigm is that it yields replicable and hence trustworthy, quantifiable research findings using rigorous well-established processes (Creswell & Creswell, 2018). Quantitative measures are suitable for conducting studies that require assessment or direct comparison of evaluation outcomes with baseline data but are also often used for positivist explanatory studies (Creswell & Creswell, 2018). Data collected quantitatively is considered to be objective because it is in the form of numbers and, hence, it can easily be analysed using statistical procedures that provide replicable findings (Wahyuni, 2012). Findings of a quantitative study can be verified in other contexts and situations related to the studied context and are generalisable to populations that are reasonably similar

(Wahyuni, 2012). A major benefit of the quantitative approach is that it is a fairly cheap, quick and easy way of data collection and particularly where data is collected either automatically or via online surveys it reaches participants easily (Wahyuni, 2012).

The disadvantage of quantitative research

The problem with the quantitative approach begins when the phenomena being studied are challenging to quantify or measure because not everything is quantifiable (Creswell & Creswell, 2018). Quantifying challenges can lead to missing valuable data that is essential to the research (Creswell & Creswell, 2018). Another drawback is that while research findings can indicate how many participants checked a particular box, it is unknown what factors influenced the participants' decisions or how they felt about the response (Du Plooy-Cilliers et al., 2014). This is due in part to the lack of 'why' questions included in quantitative research. Where space is provided for additional comments in questionnaires, the respondents very often leave them blank and the data from comments may be too brief or poorly articulated. Another significant challenge for quantitative studies is a low response rate particularly when surveys are to be completed online (Creswell & Creswell, 2018). Some participants might decide not to complete the questionnaires because this method depends only on them for data collection (they feel no obligation to the person who is doing the research or who is actively supporting the research effort) (Creswell & Creswell, 2018). The main shortcoming of the quantitative technique, according to Myers (2013), is that it has the tendency to view human behaviour independently of the context of the study which can also result in over-generalisation. In addition, the occurrences are taken out of their natural world context, they rely on accurate or truthful and thoughtful input. Also, it relies on the research design; the impacts of variables not included in the model are ignored (Myers, 2013).

Justification for quantitative study

The aim of this study to evaluate cyber-security controls' effectiveness in the DHIS. Therefore, a sufficient number of participants were needed to submit the data used to reach conclusions about the effectiveness of cyber-security controls. In other words, the researcher required input from a diverse population of people who use the DHIS system. The quantitative method was helpful as the research used a questionnaire to collect data. Collected quantitative data were analysed and then presented in charts, tables and graphs and as statistical values, making it

relatively easy for the researcher and readers to see and understand patterns. This survey used self-reported data, that is, it relied on respondents to give accurate input, but the questions relied on recollection of past events and to an even greater extent, on perceptions.

Statistical data analyses were used to test the formulated hypothesis to discover meanings and determine the findings. In addition, the researcher aims to determine the cause-and-effect linkages between numerous factors by accepting or rejecting the hypothesis developed for the study.

4.6.2 Qualitative research approach

Qualitative research is an approach where the researcher seeks to understand and explore the meaning that different groups of people or individuals who are directly impacted by a particular problem being solved ascribe to a sequence of events (Creswell & Creswell, 2018). According to Creswell and Creswell (2018), one aspect of the qualitative research approach is creating questions and procedures to explore or study a topic in depth. The research problems and questions serve as a guide for the inductive approach, which is utilized to collect evidence that will be used to construct a plausible explanation as to why things happen (Saunders et al., 2019). Typically, interviews are conducted to collect information from individuals who are actively involved in or impacted by the research environment (Saunders et al., 2019). Furthermore, inductive analysis is used to analyse the data, and the researcher then interprets the findings (Saunders et al., 2019).

Increased knowledge of human behaviour, attitudes, experiences, and intentions is the goal of the qualitative approach (Saunders et al., 2019). This may be accomplished by watching (in field studies) or interviewing participants and analysing the various actions and textual input obtained from research study participants (Creswell & Plano, 2011). Qualitative research design obtains words (text) to express the participant's the meaning of a situation, and the interview questions are open-ended to allow the participants to express their recollections of experiences, opinions as to why certain things were done or happened (Myers, 2013). The focus is on qualitative (textual) data, which examines the experiences, convictions, ideas, behaviours, and motivations of participants (Saunders et al., 2019). Focus groups, observations, interviews,

and personal document analyses are typical qualitative research methods (Saunders et al., 2019).

Advantages of qualitative approach

According to Saunders et al. (2019), the qualitative approach is considered to be helpful for researchers to comprehend the meanings people assign to social phenomena and to explain the processes of human behaviour. Results produced are rich and detailed, which is the qualitative approach's main benefit (McGregor, 2019). The participants' viewpoints and the context are considered to be of utmost importance for understanding underlying behaviour of individuals and groups acting alone or as teams (McGregor, 2019). Qualitative method focuses on the 'why' of the inquiry (McGregor, 2019). Participants' opinions, beliefs, experiences, references, and thoughts are covered in the subjective interpretivist research (Saunders et al., 2019). This allows the researcher to gain a deep understanding of the study.

The disadvantage of the qualitative approach

Qualitative data's significant disadvantage, according to opponents is that it is subjective (McGregor, 2019). Due to this subjectivity, there may be bias and false information (Myers, 2013). Another drawback is that gathering data and conducting analyses usually takes a long time and may be difficult (McGregor, 2019). The researcher's choices of codes and categories are the primary scaffolding and qualitative content analysis takes a lot of time (McGregor, 2019). Data statistical analysis may not be used because qualitative data has a small sample size, and conclusions may not be generalisable to other contexts and circumstances (McGregor, 2019). Due to the aforementioned factors, a qualitative approach will not be appropriate for this study.

4.6.3 Mixed methods

Another approach is mixed method, which includes simultaneously collecting quantitative and qualitative data. In mixed methods, the researchers carry out the inquiry assuming that collecting different data types will give them a clearer understanding of the research problems than when one approach is used (Saunders et al., 2019).

4.7 Research strategy

The numerous forms of inquiries from mixed methodologies, quantitative, and qualitative approaches that give the methods used in research design are examined by research strategy (Denzin & Lincoln, 2011). The survey research strategy was used to collect, analyse and interpret quantitative data for this study. The choice's justification is discussed below.

4.7.1 Case study

A case study research strategy explores a phenomenon within the context of its real-life situation by observing inquiries of the problem and objectives of the research (Creswell & Creswell, 2018). Case studies are usually used when an in-depth investigation and holistic approach to individuals or groups are explored within the research context (Creswell & Creswell, 2018). Case study research can be based on one or many cases and is usually suitable for a qualitative approach (Yin, 2003). When using a case study, one needs to look at three main categories of studies: exploratory, explanatory, and descriptive (McGregor, 2019). Exploratory case studies seek to explore and answer questions on how a particular occasion happened, why it happened, and the obvious uniqueness of this event or circumstance (Zainal, 2007). Descriptive case studies simply seek to describe in detail the phenomenon happening within the inquired data (McGregor, 2019). During the descriptive case study, researchers aim to describe occurrences and phenomena as they occur in the context of the study (McGregor, 2019). Questions on "who" and "where" are answered in this strategy (Zainal, 2007). Finally, explanatory case studies are the most complex as they aim to shed light on a phenomenon (McGregor, 2019). An explanatory case study strives to convincingly describe the case using the facts, thoughts on potential explanations, and reach a conclusion focused on descriptions that are trustworthy and consistent with the facts (Yin, 2003). Explanations for the "how" and "why" are explained during this strategy (Saunders et al., 2019).

4.7.2 Survey design

Positivist surveys use questionnaires as a data collection instrument (McGregor, 2019). In this case, the survey design strategy provides a numeric description of variables of a chosen population by randomly studying a sample of the entire population (Saunders et al., 2019).

However, some researchers use structured interviews to collect data in the survey strategy. An example might be telephone surveys or facilitated surveys where the facilitator interviews respondents one at a time and fills in the questionnaire one question at a time but converting the verbal response into a single number representing of the options on the data sheet.

Creswell and Creswell (2018), define a survey as a strategy that describes a selected population's opinions, trends, and attitudes. They further explain that a survey provides tests associated with the demographic variables of a population and use descriptive statistics to analyse the data (Creswell & Creswell, 2018). It is important to note, however, that surveys making use of questionnaires are often used in positivist explanatory research as described in Section 4.2.1 and use inferential statistics to analyse the data. According to (Saunders et al., 2019), a survey is mainly used in quantitative research.

Data collection during the survey may be cross-sectional or longitudinal (Saunders et al., 2019). Cross-sectional data collection occurs at one point in time (sometimes called a snapshot), and longitudinal data collection happens over time which would require a series of data collection sessions (Saunders et al., 2019).

Researchers are able to collect data from a large number of respondents (McGregor, 2019). Participants can be given questionnaires which they complete unassisted, which makes gathering primary data more feasible and more economical (McGregor, 2019). If this is the modus operandi, large amounts of data can be collected at low cost from a sizeable sample and the collection is done quickly (Ranjit, 2019).

The survey strategy is mainly used to answer questions such as where, what, how, and who (Ranjit, 2019). Therefore, this strategy is frequently used for descriptive and exploratory research. Collected data are easy to understand and interpret and can be analysed using statistical methods (Ranjit, 2019). Results of a survey can be generalised to the entire population of that study (Ranjit, 2019).

Justification of the survey design

The survey research strategy was suitable for this study because it allowed data to be collected from many respondents in a short period of time. The population of this study was people who work in healthcare. This population is usually very busy with patients; therefore, distributed

questionnaires was an easy way for respondents to participate. Furthermore, using quantitative analytical techniques, the researcher can arrive at conclusions based on relationships between variables from analysed data.

Creswell and Creswell (2018) are of the opinion that researchers evaluate variable relationships extensively when using surveys. They further point out that this extensive, and sometimes excessive, study of variables is impossible in laboratory or field experiments observations (Creswell & Creswell, 2018).

It is important to note that while a survey was suitable for this study, it also has some weaknesses. One of the main weaknesses of surveys is that it might be challenging to gain a more nuanced view including insights related to the processes or unidentified causes in the sequence of events being measured (Louis et al., 2007). Inadequate responses brought about by respondents' self-administration of questionnaire responses might also be a shortcoming (Creswell & Creswell, 2018). Another frequently encountered disadvantage of the use of questionnaires is the low response rate. Quantitative data online collection process using a structured questionnaire as an instrument can be difficult to control as the research does not have direct contact with and hence does not influence respondents to complete the questionnaire. The researcher attempts to overcome the challenge of a low response rate by making numerous follow-ups with the participants to get a high response rate. Due to the respondents' independence and lack of concern about the identity they may complete questionnaires quickly and carelessly, and hence data collected using questionnaires might not be accurate (Saunders et al., 2019).

Saunders et al. (2019) argued that it is not difficult to obtain quantitative data, which is more concise. Survey method was also chosen because it was effective and affordable (Saunders et al., 2019). In addition, this made it possible to limit the study to a representative sample of the intended study's target population. Furthermore, the survey design is thought to be more appropriate for this study based on its methodology, philosophical presumptions, and interpretive approach.

4.8 Time horizon

A time horizon emphasises a schedule of events related to the research and occurring when the research is conducted (Ranjit, 2019). There are two types of time horizons: longitudinal and cross-sectional (Creswell & Creswell, 2018). Longitudinal time horizons are repeated activities such as data collection and are done over an extensive period because the researcher wants to observe the changes or developments in specific designs in the phenomenon being reviewed (Saunders et al., 2019). Hence there may be iterations or cycles of data collection and analysis to address gaps or errors identified or the cycle may be investigating the influence of uncontrollable external events in the progress of a phenomenon. In contrast, cross-sectional time horizon studies are conducted when the researcher has limited time (Saunders et al., 2019). According to Saunders et al. (2019), in this case observations occur over a short period. This study adhered to the cross-sectional time horizon because it was carried out for academic objectives within a pre-set time frame.

4.9 Research population

The collection of persons, groups of people, or items that meet the requirements of the research setting and have the same features is known as the research population (Webb & Auriacombe, 2006). Hence, the research population is the total set of objects, people, or groups that the study is focused on and from which samples can be extracted for examination. The target population, also known as the theoretical population, consists of all the individuals and groups of objects from which the researcher will collect data (Creswell & Creswell, 2018). A reasonably large group of participants can help the researcher discover the required information (Asiamah, Mensah & Oteng-Abayie, 2017). The research population is usually large, not easily manageable, and its sampling is also difficult (Saunders et al., 2019). Target population should be defined precisely because its description will determine whether the sampled cases are appropriate or not for the survey (Bartlett, Kotrlik & Higgins., 2001). Temporal and geographical features of the targeted population should be outlined, including the type of units (Asiamah et al., 2017).

This study aims to determine the effective ways of encouraging compliance with the District Health Information System (DHIS) cyber-security controls by examining how healthcare

support staff from the Tshwane District Healthcare Centres who interact directly with the DHIS perceive ICT threats. The underlying assumption made is that cyber-security controls will only become fully effective as a means to prevent cyber-threats in healthcare centres if the people interacting with the DHIS are motivated to adhere to those controls and then consistently act in accordance with the prescribed processes and procedures.

An accessible population for this study were individuals who have access to the DHIS at Tshwane District Healthcare Centres. The decision to accessible population was based on geographical barriers and time constraints. It was intended that, in order to acquire pertinent data for the study, it would be confined to individuals who have experience with the DHIS system. Only employees who use the DHIS system in Tshwane Healthcare Centre on different levels, such as Data capturers, Information clerks, ICT administrators, Facility Information Officers, Facility Information Managers, District Information Managers, Heads of the departments, were considered.

4.10 Sampling techniques and sample size

Sampling is when a porting of population is selected, and this population is used to represent the whole population (Bartlett et al., 2001). In addition, sampling is an important element in the research process because the researcher must carefully take into account the resources they have at their disposal and time restrictions (Creswell & Creswell, 2018). Finding a representative or generalizable sample is difficult (Creswell & Creswell, 2018). Probability sampling and non-probability sampling, the two primary types of sampling, are briefly reviewed (Daniel, 2012).

4.10.1 Probability sampling techniques

The technique of probability sampling is a collection of methods that reduces the researcher's partiality and is more generalisable (Daniel, 2012). It allows the researcher to use random sampling techniques to create a sample (Creswell & Creswell, 2018). The researcher must ensure that different units from the population have exactly equal probabilities of being chosen (Bartlett et al., 2001). According to Creswell and Creswell (2018), data analysis of probability sampling results has a higher chance of accurately reflecting the entire population (Creswell &

Creswell, 2018). Probability sampling has four main categories: simple random, systematic random, stratified, and multi-stage cluster (Daniel, 2012). The probability sampling technique will not be suitable for this study as participation needs to be voluntary and this reduces the number of suitable people available. Therefore, random techniques will not be used to draw samples - the researcher wishes to include anyone available at the study time.

4.10.2 Non-probability sampling techniques

The non-probability sampling technique is a technique that does not use a random method to draw the desired samples (Bartlett et al., 2001). This sampling technique depends on sensible decisions but also takes into account practical constraints to draw samples (Bartlett et al., 2001). The researcher chooses participants that are easily accessible (Bartlett et al., 2001).

Justification for non-probability sampling

A non-probability sample was considered to be acceptable in this research. This decision was made in accordance with the study's goals, which include testing an explanatory hypothesis. Hence, it used a quantitative research methodology and non-probability sampling (Daniel, 2012). A primary reason for the choice was the study's constrained time and financial resources. This study employs both convenience sampling and purposeful sampling. Therefore, not every DHIS user in the Tshwane healthcare facilities had an equal probability of being chosen for the sample. The researcher's inability to get an entire list of every district user of the DHIS is one cause of this and potential study participants were challenging to reach. Therefore, the researcher argued that sampling must be done using a non-probability sample rather than a random sample.

Four main categories fall under non-probability sampling and are briefly explained below: convenience, snowball, quota, and theoretical (Daniel, 2012).

Convenience sampling

Convenience sampling, also called availability sampling, is a method of non-probability sampling (Bartlett et al., 2001). Only the available people can be conveniently selected by the researcher to take part in the study during data collection (Daniel, 2012). Easily accessible and nearby participants are taken as the first available primary data source since there are no

additional requirements (Daniel, 2012). Any participant who met the inclusion criteria was therefore asked to participate in the study.

Justification of convenience sampling technique

This study followed convenience sampling and purposive sampling techniques. The initial study population were users of DHIS at Tshwane district's healthcare centres, but this population is not always easily accessible as they are always busy. The convenience sampling choice was based on the researcher selecting the most relevant available participants during the study. Convenient sampling was suitable since the researcher only collected data from the participants who volunteered or agreed to participate in the study. In this study, the employees who use the DHIS system in Tshwane Healthcare Centre on different levels, such as data capturers, information clerks, ICT administrators, Facility Information Officers, Facility Information Managers, District Information Managers and the Head of the Department, were selected.

Purposive non-probability sampling

In purposive sampling, the researcher chooses research respondents from a specific population because they fit the study's purpose (Creswell & Creswell, 2018). For the purpose of this study, the inclusion sampling criteria was based on users of DHIS who have access to the system. Participants who matched the inclusion criteria of this study were selected to participate in the survey purposely. As a result, participants who use the DHIS system were regarded as the study's population sample. However, the sample was drawn only from readily available participants and the sample was both purposive and convenient. Participants included employees of Tshwane Healthcare Centres who are familiar with and use the DHIS system. The sample was selected regardless of gender, age, or race. Employees using the DHIS system in Tshwane Healthcare Centre include data capturers, Information clerks, ICT Administrators, Facility Information Officers, Facility Information Managers, District Information Managers, and heads of departments.

4.11 Data collection procedure

A researcher must gather data from relevant sources to answer the identified research problems and questions, test hypotheses, and assess the outcomes (Creswell & Creswell, 2018). Two types of data collection procedures are primary and secondary data collection (Creswell & Creswell, 2018). Primary data is obtained directly from the participants and has not been used before (Creswell & Creswell, 2018). It is regarded as the original data. In contrast, secondary data collection has been organised, analysed, and used by other people prior to the study, and those results might have been published (Creswell & Creswell, 2018). Secondary data is, therefore, 'second-hand' data and might be obtained from open-access data repositories. Secondary data is, therefore, readily available data (Creswell & Plano, 2011).

Primary data that had not been collected or analysed before were required for this research. Primary data collection was chosen because secondary data collection might not fit the requirements of the intended research well or might not be reliable depending on the source and reputation of the original researcher (Pallant, 2020; Awabil & Anane, 2018).

Primary data was collected at Tshwane District Healthcare Centres using online questionnaires as a collection tool. The questionnaire tool consisted of 21 compulsory and closed-ended questions that enabled the respondents to select the answer. A Likert scale of 1 to 5 was used in the questionnaire for questions 8 to 17, with 1 being strongly agreed and 5 strongly disagree. Data was collected directly from the individuals and sent by them individually to the researcher. A total of 160 participants were invited to participate in the study and 126 questionnaires were completed and returned. Microsoft forms were used to create and administer the data-gathering instrument. The Microsoft link was shared with participants via e-mail, WhatsApp and SMS text messages. The questionnaire was anonymous, and the private details of respondents were not collected, although a small amount of relevant demographic data was collected.

As previously mentioned, participants were selected using purposive and convenience sampling, and their contact details were obtained from the Tshwane health district facilities manager. This study's respondents were anonymous. For this study, where respondents were workers who handled patients' private information, anonymity was crucial. Since questionnaires were filled out without the researcher's involvement, the response was unaffected by outside influence and depended entirely on the respondent as to the amount of

attention given to the process. Unlike sitting and doing face-to-face interviews, questionnaires allowed respondents to complete the survey conveniently while saving the researcher's time.

4.12 Data analysis

Data analysis is when the researcher reviews, cleanses, transforms, and models the collected data (Ranjit, 2019). Quantitative data analysis was done to determine the information and get valuable evidence for inferences, and it was helpful when making decisions (Ranjit, 2019). The data analysis was done so the researcher could completely understand what the findings indicate or mean (Pruzan, 2016).

When the data collection was completed during the study, the data was captured and structured in a Microsoft Excel spreadsheet. Then this data was stored on a software package for quantitative analyses, the Statistical Package for Social Sciences Statistics (SPSS) version 26. Once the data was analysed, report findings were generated based on the data. The data was analysed using multilinear regression to offer quantitative evidence of the effectiveness of cyber-security controls in DHIS.

Exploratory Factor Analysis was used to test and analyse the factors and check if the questionnaire tool was valid. Validity was achieved by following five steps of measurement. These steps were undertaken using the Kaiser Meyer Olkin (KMO) and Bartlett's tests, Communalities test, Total variance explained, Scree plot, and Factor Rotated Component Matrix. The factor analysis determines if the variables employed accurately measure the concept. The Bartlett test was used to analyse whether there were any significant correlations between variables. The Communalities test was used to analyse the amount of variance counted for each variable for all factors and components for correlation purposes. Rotated components matrix analysis was used to determine how well items were associated with their parent factor. Reliability analysis was conducted to evaluate the degree to which the factor's measurement is trustworthy and consistent. Cronbach's Alpha was used to analyse the internal consistency of these choice variables. The reliability test was done in this study to find relationships between variables.

Furthermore, item analysis was used to evaluate the internal consistency of these decision variables for each item on the questionnaire (Hamid et al., 2011). Additionally, reliability was

used to assess the relationship between a factor and a set of items, and the Cronbach Alpha coefficient (α) was used to determine the scaling (Heo, Kim & Faith, 2015). The researcher performed additional analysis using descriptive statistics to determine the Mean, Standard Deviation, and Frequency for each item of the questionnaire's factors. To assess the data's normality across all factors or items, descriptive statistics were computed. In order to test the hypothesis, regression analysis was lastly used to model ad hoc relationships. A numerical summary of the strength and direction of the linear relationship between two variables was provided by correlation analysis. In this study, correlation was measured using Pearson's correlation analysis (Cohen, Manion & Morrison, 2007). The analysis determined whether the factors among Technology Threat Avoidance factors, the TOE factors and the Technology Acceptance Model had a statistically significant relationship.

4.13 Validity and reliability

Reliability: The researcher concentrated on the identified research problem in order to answer these questions. It is found that the research design is an essential tool for assessing the reliability of the analysed data. The measurements determine how accurate the method is for measuring data (De Vos et al.,2009). Instruments that are used for measurements must be able to provide reliable numerical results every time it is used. Greenfield, (2002) indicated that the reliability of the question is when participants provide the same answer in various instances. Results must not vary, except if there are differences in the variables that are being measured. It does not change unless there are variations in the variables being measured.

Validity: To ensure that the study is valid, the researcher concentrated on the purpose of the study and research questions so that there is certainty that facts be discovered in finding evidence of the study. Validity is the rate or extent at which the tool can do what it is supposed to do (De Vos, Strydom, Fouche & Delpont 2009), and research questions measure what they say they measure (Greenfield, 2002).

Internal validity is highly dependent on the study procedures and if the study is performed carefully and thoroughly (De Vos et al.,2009). Internal validity considers the degree of confidence that the survey findings are trustworthy, avoids traps that make the outcomes questionable, and is not influenced by other variables or factors.

External validity is when the study's conclusions can be accurately generalised to a broader context. This means that the researcher should be able to reasonably generalise the study findings to other people, groups, measures and situations directly impacted by the results and share similar characteristics with the selected sample. The research design is an online, anonymous questionnaire; therefore, the researchers know no internal or external factors impacting the research design.

Construct validity: To assess the validity of the instrument, the researcher used Exploratory Factor Analysis (EFA). Constructs (referred to as factors throughout this dissertation) and the validity of the questionnaire tool were tested using the EFA. To determine validity, the researcher followed five steps. Kaiser Meyer Olkin (KMO) and Bartlett's tests, the Communalities test, the Total Variance explained, the Scree plot, and the Factor Rotated Component Matrix were used.

The validity of the questionnaires was also ensured using an appropriate process for drafting questions – a well-balanced sample questionnaire related to the research topic and ensuring that the findings come from the collected and analysed data. Reliability of the data was ensured in that if the same questionnaire is given to the same respondents would yield the same results. Alternatively, distributing the same questionnaire in two parts to the same respondents would result in the same score. When possible, reliable studies use random samples, make use of appropriate sample sizes, avoid biases, and are carried out by researchers who are not swayed by funding or the need to achieve particular outcomes.

4.14 Research limitations

Certain restrictions may also affect how the study is conducted in all initiatives. Limitations are flaws, influences, or circumstances that undermine the findings of the research (Saunders et al., 2019). These limitations are out of the researcher's control and have constraints on the outcome and methodology. Limitations or restrictions are numerous, but they are associated with the process of undergoing any research (Creswell & Creswell, 2018). Accumulation of data could limit the study in many ways: time, access to the population, and cost constraints. Time restrictions relate to the amount of time available to gather the data needed for output. UNISA due dates constrain and limit the amount of time that can be used to examine issues

raised in the research or assess changes and developments over time. Employees of the Tshwane district healthcare facilities and primary healthcare professionals who regularly use the DHIS system were required to participate in the study. This is another limitation since the population targeted is mostly busy and works with sensitive data. Geographical barriers were also a limitation of this study since data cannot be collected in all healthcare facilities. However, due to financial and time limitations, this study was only able to include healthcare members who were Tshwane district municipality residents and lived in Pretoria. This study only included residents of Tshwane, and the output could be applied broadly.

Furthermore, the study assumed that the people in Tshwane district healthcare have the same experience using the DHIS systems as other users have in other parts of the country. Therefore, it was expected that the data collected from participants in Tshwane district healthcare would reflect the experience that other users have in other parts of the country. Hence, it facilitated the generalisation of the study findings in similar situations.

4.15 Ethical considerations

In their book, Saunders et al. (2019) define ethics as how appropriate the researcher's behaviour is regarding the rights of those affected by the study or who become the subject matter. Ethics occurs to give the foundation that pursues to handle questions about morals (Recker, 2013). It includes concepts such as whether something is bad or good, right or wrong, whether justice is applied, and virtue (Recker, 2013). Ethics describes what is viewed as the right or wrong thing to do in a profession or community and can serve as a guide for free moral agents on how to act (Recker, 2013). According to Pruzan (2016), ethics are the standards and norms that demonstrate the researcher's decision regarding their interactions with other people and their behaviour. They went on to say that moral behaviour and decision-making are aspects of ethics (Pruzan, 2016).

Bryman and Bell (2015) stated that some methods need more emphasis on ethical consideration than other options. Like various observations that require higher consideration in the construction of questionnaires or obvious ethnography that can give the impression of being safe from ethical problems (Bryman & Bell, 2015). These impressions do not have a base, particularly when looking at the main four areas: lack of informed participants, harm to

participants, deception, and invasion of privacy (Bryman & Bell, 2015). Questioners do not allow or give a chance to cause such ethical problems since the researcher does not necessarily need to be there when participants answer questionnaires, unlike in observations or interviews (Saunders et al., 2019). This study used a questionnaire that respondents completed independently, giving them total anonymity.

Furthermore, the first page of the questionnaire had information that described the survey's aim and informed the respondents that the survey would be treated as anonymous (Saunders et al., 2019). The researcher's contact details in the event the respondents had any questions regarding the survey were also provided. Participants were provided with the section to consent before participating in the study. Informed consent is a voluntary agreement to participate in research. Participant goes through a process where they comprehend the study and its risks. Before enrolling in the study, participants must sign an informed consent form, which must also be followed up on after they've signed up. Informed consent gave the participants what the study was about and adequate information about the research and ensured that the participants understood this information. It gave reasons why the researcher was collecting data and why they were participating in the study. Lentz et al (2016); Manti & Licari (2018) added that it gave the participant the option to volunteer for participation in the study and allowed for withdrawal. UNISA have a clear policy that protects human participants and ethical standards acceptable when conducting a study involving humans. Therefore, the researcher used UNISA's ethics policy to guide human participant involvement. Ethical clearance was applied with the UNISA School of Computing Ethics committee, and approval was granted before data collection. Furthermore, the Tshwane research committee permitted access to participants at the Tshwane District Healthcare Centres.

Every research where there is human involvement has specific ethical issues. The researcher looked at the following ethical issues concerning data collection to not affect participants.

- Participation – Participation in the study was entirely voluntary. No participant was forced to take part in the survey. All participants were fully informed that taking part in the study is one's choice.
- Withdrawal – Those who chose to participate were allowed to withdraw anytime before submitting their questionnaire. Participants were well informed that they had the right

to change their minds about participating in the study if they had not submitted their questionnaires. This was because the online survey was anonymous, and once the participants submitted their survey, the researcher could not know which questionnaire was completed by who. Therefore, the researcher couldn't withdraw any participants at that stage. Participants were well informed about the timeframe to withdraw from the study if they wished to.

- Informed consent – The collection of data was done through an online questionnaire. Participants gave the researcher consent to participate in the study. All the essential information about the study was on the online questionnaire. By proceeding with the survey, participants automatically gave consent to participate in the study. The researcher provided a clear indication of the purpose and nature of the study. All study features were communicated to participants to allow them to decide on being part of the study.
- Anonymity – The identity of participants was kept confidential and safe. The study did not collect any personal details of participants. Once the participant submitted the questionnaire online, the researcher could not identify who submitted which questionnaire.
- Confidentiality – It was the researcher's responsibility to keep all information from the participants about the study as confidential as possible and only disclose it to the relevant people.

Ethical report – The researcher did not provide false information about the study. They did not leave out any information collected from participants or distort any findings. Results were reported accurately and honestly.

4.16 Sample size

The designated sample is the total number of sample elements the researcher chose for data collection (Bartlett et al., 2001). The final sample size is the total number of interviewed participants or elements that data was collected from (Bartlett et al., 2001). It is not simple to decide how small or big the sample size should be, as this depends on numerous considerations (Bartlett et al., 2001; Daniel, 2012). Two practical factors that are important in affecting the

sample size decision are time and money (Daniel, 2012). Therefore, the sample sizes of studies are a compromise between the ideal calculated mathematically and those two factors.

Employees of Tshwane district healthcare facilities who used the DHIS system made up the study's population. The Tshwane district has 83 healthcare facilities, including 11 hospitals, 8 Community Healthcare Centers (CHC), and 64 Clinics. Not all healthcare facilities use the DHIS system, which is why those were left out of the study. The Gauteng Department of Health authorised the visitation of 37 healthcare facilities. There are about 332 people in the population who have access to the Tshwane Healthcare centers' DHIS system. The researcher set the target sample to 160 respondents, but these were not divided into representative groups of set sizes. The Kaiser Meyer Olkin (KMO) test was used to determine if the sample size utilised in a study was adequate for Factor Analysis (Awabil & Anane, 2018).

4.17 Chapter Summary

The research methodology chapter outlined the methods followed in this study. The sections covered in this chapter are the philosophical assumptions guiding the research. The research approach followed, which is quantitative, was also covered. Furthermore, the chapter discussed the data collection and analysis of the study. The following chapter will discuss the data analysis. Lastly, ethical consideration was also given as it is an important aspect of the study.

CHAPTER 5: Data Analysis and Interpretation

5.1 Introduction

The influence of a variety of factors in motivating users who were interacting directly with the DHIS to take measures to protect the DHIS from cyber-attacks is analysed in this chapter. The chapter starts off by analysing the demographics of the participants in the research and the frequency distributions. The Exploratory Factor Analysis was used to assess the validity of the data, while Cronbach's Alpha was used to test the reliability of the data. Descriptive statistics and correlation were also investigated. Finally, regression analysis and hypothesis testing were carried out.

5.2 Response rate and data cleaning

In this study, the researcher used an online survey questionnaire. A total of 160 participants were invited to participants. The tool for collecting data was developed using Microsoft forms. A total of 126 people responded to the online survey, representing a response rate of 78.75%. Data cleaning was carried out on all 126 questionnaires received. After data cleaning, the distribution of the data was normal; there were no incorrect or missing responses. As a result, all of the surveys that were submitted by respondents and used in this study were reliable.

5.3 Demographics analysis

Demographic characteristics were determined based on gender, age, the highest level of education, and professional or administrative positions. According to the demographics (see Table 5.1), 84 respondents were females, accounting for 66.67% of the total, 36 were males, accounting for 28.57% of the total, and 6 preferred not to say and accounted for 4.76%. Age was classified into the following groups: 21 to 25 years (4.76 %); 26 to 30 years (33.33%); 31 to 35 years (23.81%); 36 to 40 years (19.05%); 41 to 45 years (11.91%); 45 to 50 years (4.76%), 51 years and above (2.38%). The demographics also looked at the respondents' highest level of education, which was classified as Standard 10/Grade 12, Certificate, Diploma, Bachelor's Degree, Master's Degree, and others in cases where the qualification wasn't on the list. The largest group 42.86% (or 54 of all respondents) had Grade 12 as their highest level of education

(see Table 5.1). Respondents with a certificate accounted for 26.19% (33), while those with a diploma accounted for (24) 19.05%. Furthermore, respondents with bachelor's degrees made up 7.14% (9) of the total. As could be expected a Masters degree had the lowest qualification percentage, with 2.38% (3), which was identical to other qualifications not specified, which also had 2.38% (3).

Table 5.1: Demographics

Gender				
	Frequency	Percent	Valid Percent	Cumulative Percent
Man	36	28,57	28,57	28,57
Prefer Not to say	6	4,76	4,76	33,33
Woman	84	66,67	66,67	100
Total	126	100	100	
Age				
	Frequency	Percent	Valid Percent	Cumulative Percent
21 - 25 Years	6	4,76	4,76	4,76
26 - 30 Years	42	33,33	33,33	38,10
31 - 35 Years	30	23,81	23,81	61,90
36- 40 Years	24	19,05	19,05	80,95
41- 45 Years	15	11,91	11,91	92,86
46 - 50 Years	6	4,76	4,76	97,62
51 Years and above	3	2,38	2,38	100
Total	126	100	100	
Highest Education				
	Frequency	Percent	Valid Percent	Cumulative Percent
Standard 10/Grade 12	54	42,86	42,86	42,857
Certificate	33	26,19	26,19	69,05
Diploma	24	19,05	19,05	88,10
Bachelors' Degree	9	7,14	7,14	95,24
Master's degree	3	2,38	2,38	97,62
Other	3	2,38	2,38	100
Total	126	100	100	

Figure 5. 1 Gender

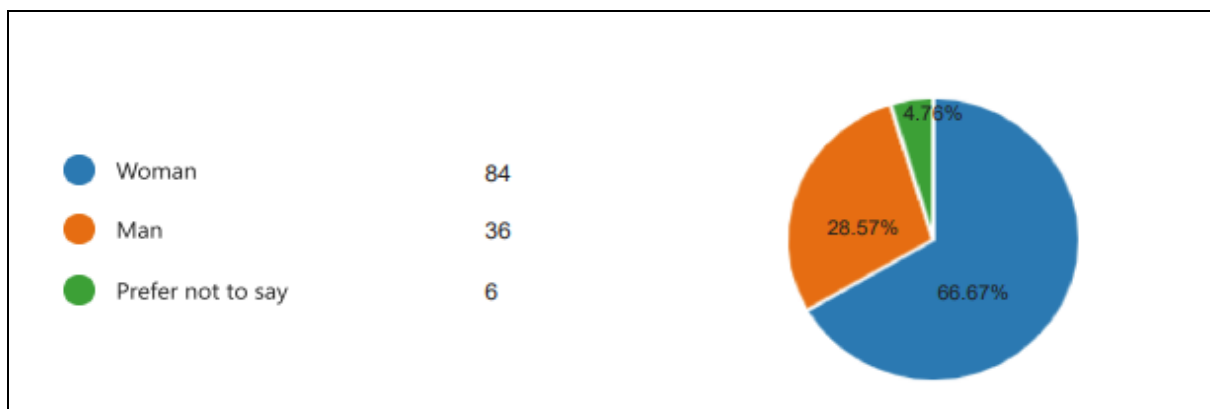


Figure 5. 2 Age group

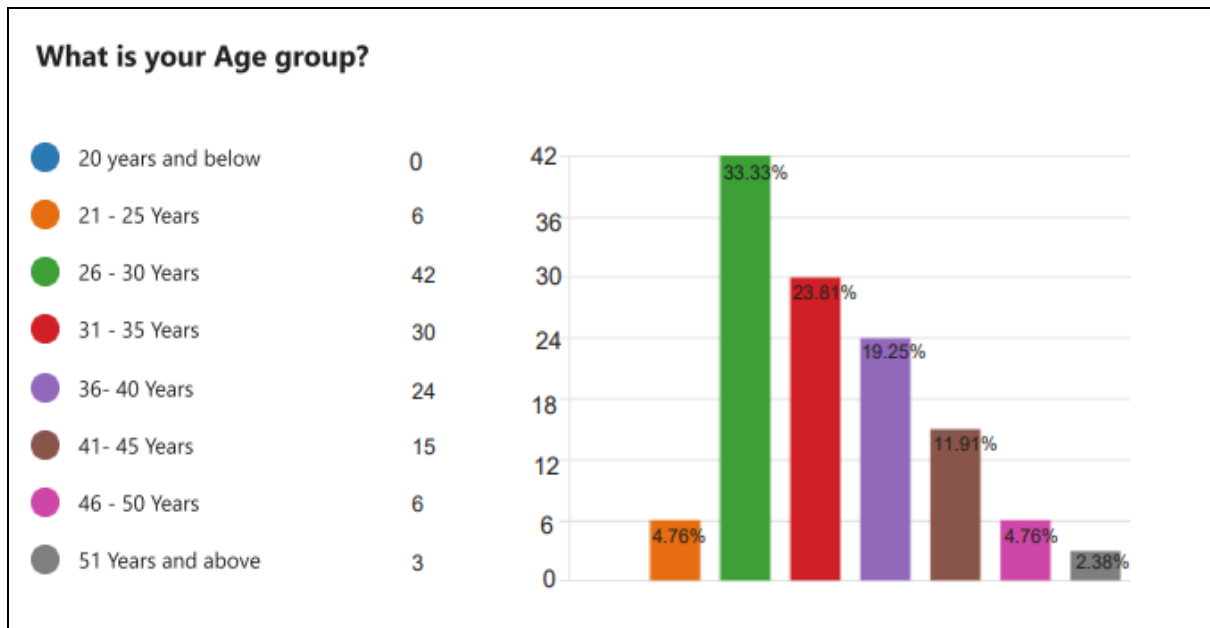
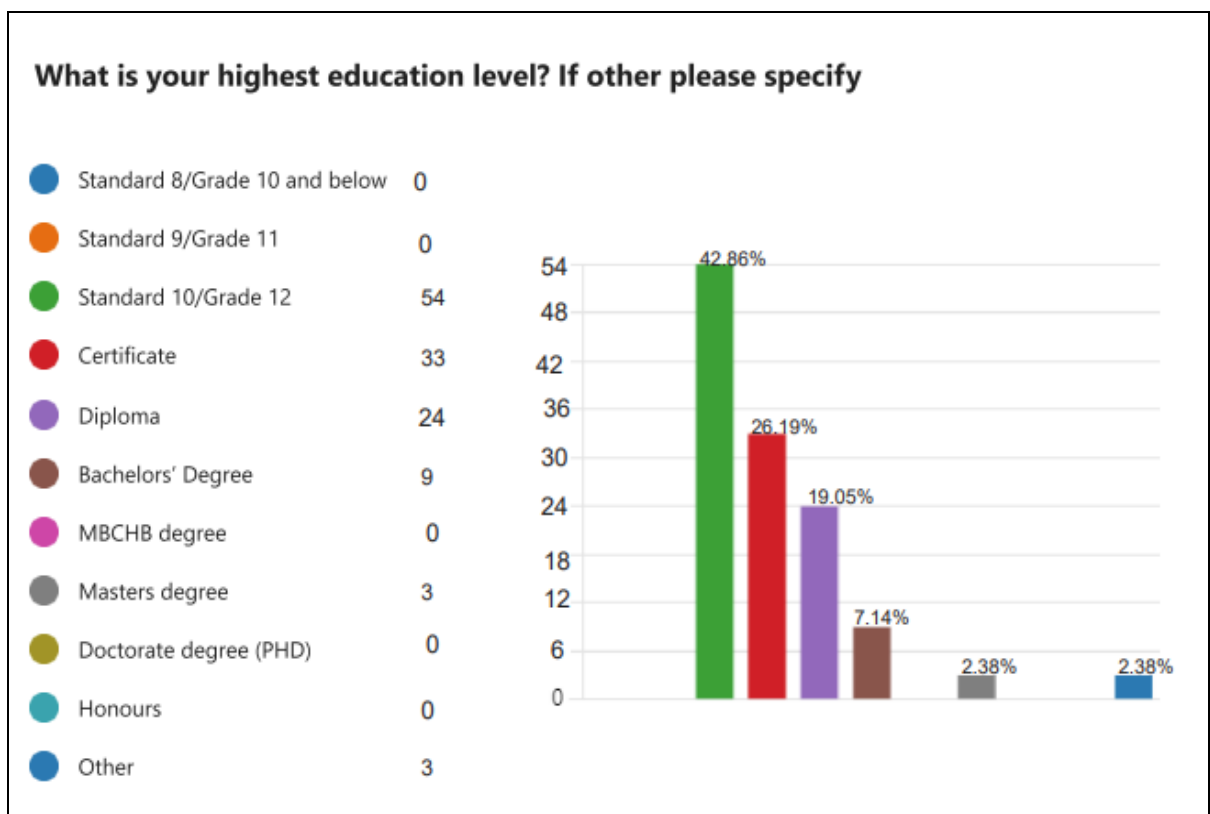
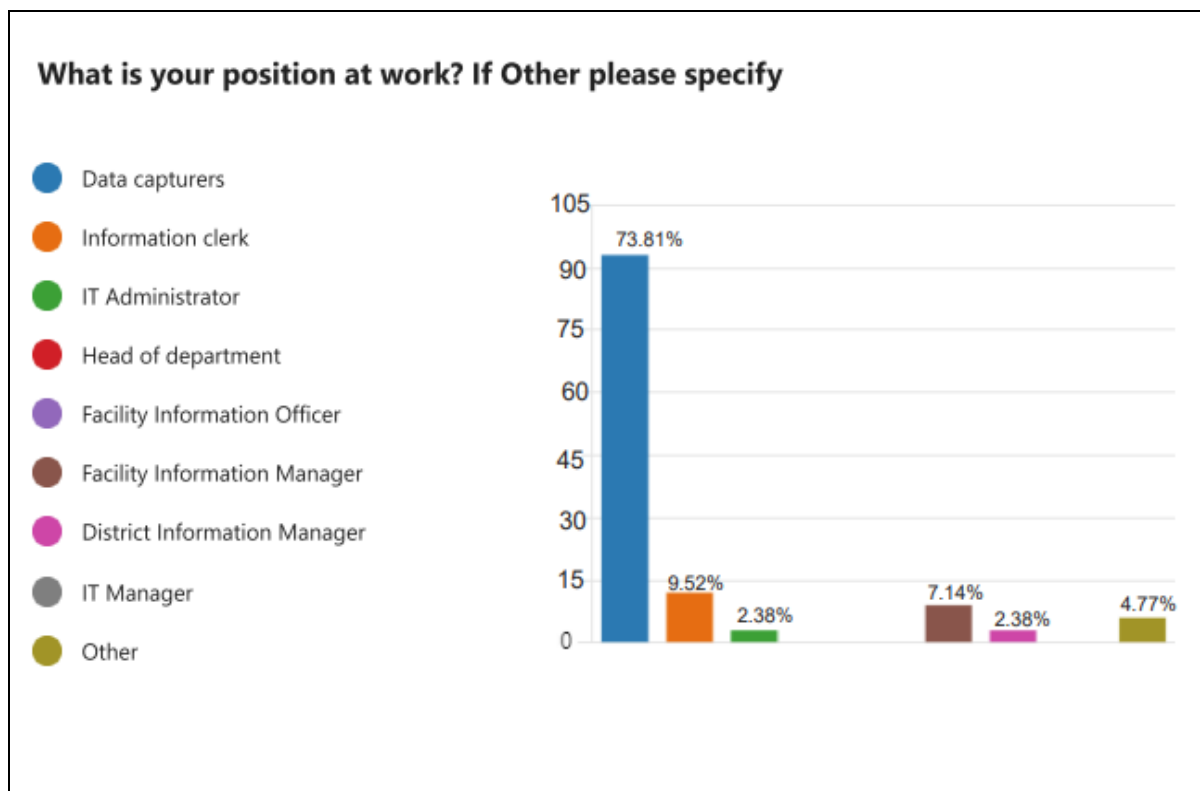


Figure 5. 3 Highest Education



Position				
	Frequency	Percent	Valid Percent	Cumulative Percent
Data capturers	93	73,81	73,81	73,81
Information clerk	12	9,52	9,52	83,33
IT Administrator	3	2,38	2,38	85,71
Facility Info Manager	9	7,14	7,14	92,85
District Info Manager	3	2,38	2,38	95,23
Other	6	4,77	4,77	100
Total	126	100	100	

Figure 5. 4 Positions



Position or occupational roles were the last demographic characteristic to be analysed. Data capturers, information clerks, IT (Information Technology) administrators, facility information managers, district information managers, and positions not specified were included. The researcher chose positions relevant to DHIS users since the study focused on users who have direct access to DHIS. Data capturers had the highest percentage 73.81% (93) (see Table 5.1). Information clerks made up 9.52% (12) of the workforce, IT administrators for 2.38% (3), facility information managers 7.14% (9), district information managers counted 2.38% (3), and other qualifications not listed counted 4.77% (6).

The sample of respondents was, therefore, mostly under 35 years of age (62%) and largely data capturers (74%). The educational qualifications of nearly 90% of the respondents were, at most, a grade 12 certificate or diploma. However, these demographic characteristics are not used in correlation analysis (Section 5.8) or regression analysis (Section 5.9).

5.4 Demographics: Information systems knowledge

Tables 5.2, 5.3, and 5.4 display the frequency distribution of the items used to gauge respondents' information system knowledge. Respondents were asked where they access the internet; and results show that 14.29 % (18) said from home, 83.33% (105) said from work, and only 2.38% (3) from internet cafés as shown in Table 5.2.

Table 5.2: Information System Knowledge (Internet Usage)

Internet				
	Frequency	Percent	Valid Percent	Cumulative Percent
Home	18	14,29	14,29	14,29
Internet cafe	3	2,38	2,38	16,67
Work	105	83,33	83,33	100
Total	126	100	100	

Figure 5. 5 Internet usage

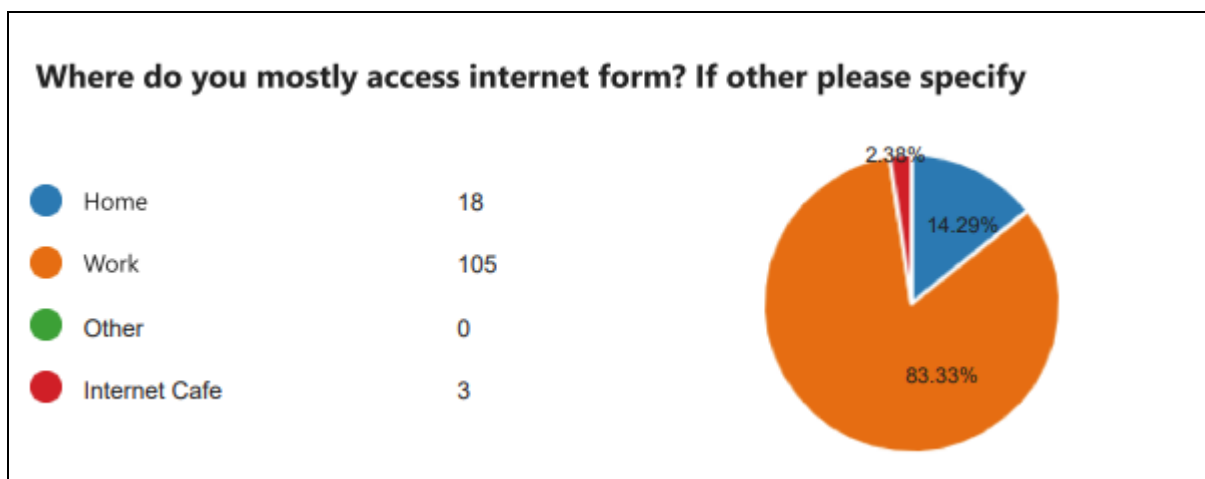
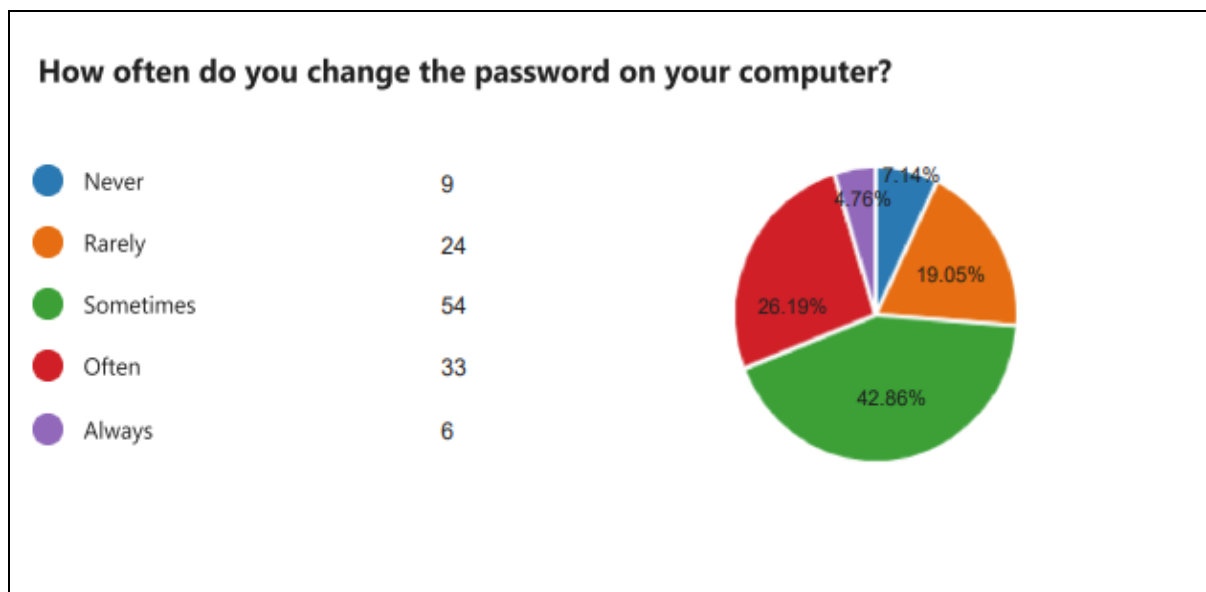


Table 5.3: Information System Knowledge (Password Change)

Password		Frequency	Percent	Valid Percent	Cumulative Percent
	Always	6	4.76	4.76	4.76
	Never	9	7.14	7.14	11.90
	Often	33	26.19	26.19	38.10
	Rarely	24	19.05	19.05	57.14
	Sometimes	54	42.86	42.86	100
	Total	126	100	100	

Figure 5. 6 Password change



The questions on changing passwords were asked to evaluate the susceptibility (or vulnerability) of users in terms of allowing cyber-criminals to gain access to DHIS. Results of this test showed that 42.86 % (54) of participants change their passwords sometimes. Only 26.19% (33) said they often change their passwords, while 19.05% (24) said they rarely change their passwords. About 7.14% of participants admitted that they never updated their passwords. A very low percentage of participants, 4.76 % (6), always change their passwords.

Table 5.4: Information System Knowledge (General Questions)

Do you have access to the District Health Information System (DHIS)?				
	Frequency	Percent	Valid Percent	Cumulative Percent
	No	9	7.10	7.10
	Yes	117	92.90	92.90
	Total	126	100.00	100.00
Is the firewall on your computer enabled?				

	Frequency	Percent	Valid Percent	Cumulative Percent
No	21	16.70	16.70	16.70
Do not know	39	31.00	31.00	47.70
Yes	66	52.30	52.30	100.00
Total	126	100.00	100.00	
Are you aware of your organization's information security policy?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	36	28.60	28.60	28.60
Do not know	9	7.10	7.10	35.70
Yes	81	64.30	64.30	100.00
Total	126	100.0	100.0	
Is antivirus software currently installed on your computer?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	24	19.00	19.00	19.00
Do not know	15	11.90	11.90	30.90
Yes	87	69.10	69.10	100.00
Total	126	100.00	100.00	

Table 5.4 (Continued): Information System Knowledge (General Questions)

Is antivirus software currently updated on your computer?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	42	33.30	33.30	33.30
Do not know	18	14.30	14.30	47.60
Yes	66	52.40	52.40	100.00
Total	126	100.00	100.0	
Is antivirus software currently enabled on your computer?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	36	28.60	28.60	28.60
Do not know	21	16.70	16.70	45.30
Yes	69	54.70	54.70	100.00
Total	126	100.00	100.00	
Are you aware of cyber-attacks?				
	Frequency	Percent	Valid Percent	Cumulative Percent
No	21	16.70	16.70	16.70
Do not know	3	2.30	2.30	19.00
Yes	102	81.00	81.00	100.00
Total	126	100.00	100.00	

Participants were asked questions under the heading Information System Knowledge and general questions about cyber-security were asked. Results displayed in Table 5.4. show that almost all the participants (92.9 % or 117) responded 'yes' when asked if they had access to the DHIS. The participants were asked if a firewall was enabled on their computers. About half (66 or 52.30%) of respondents believed that was the case and they were protected to some extent against cyber-attacks. 64% of participants said they knew about the organisation's security policies. Ant-virus software knowledge was 69% knew it was installed; fewer (55%)

knew whether it was actually active; and about the same number (52%) knew whether it was regularly updated.

5.5 Exploratory factor analysis (EFA) Validity

To assess the validity of the instrument, the researcher used Exploratory Factor Analysis (EFA). Constructs (referred to as factors throughout this dissertation) and the validity of the questionnaire tool were tested using the EFA. To determine validity, the researcher followed five steps. Kaiser Meyer Olkin (KMO) and Bartlett's tests, the Communalities test, the Total Variance explained, the Scree plot, and the Factor Rotated Component Matrix were used.

5.5.1 EFA Validity Test

To determine whether there were any significant correlations between the variables Bartlett test can be used (Pallant, 2020). The Bartlett test scale has a threshold of ($p < 0.05$). When Bartlett's test yields a statistically significant value, there are sufficient correlations among the Likert scale questions to perform the factor analysis test (Bartlett et al., 2001).

5.5.2 KMO (Kaiser Meyer Olkin) and Bartlett's test

Table 5.5 shows statistical data for KMO (Kaiser Meyer Olkin) and Bartlett's test. As indicated, the KMO value for testing sampling adequacy was 0.736, which was greater than 0.5. This value met the KMO test's validity criteria (> 0.5), as recommended by Pallant (2020). Furthermore, Bartlett's Test of Sphericity had a significance level (p-value) less than 0.05. It was reasonable to undertake the Factor Analysis test for this reason. The results of the KMO and Bartlett tests thus demonstrated a suitable correlation between variables for conducting EFA.

Table 5.5: KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.736
Bartlett's Test of Sphericity	Approx. Chi-Square	171.46
	Df	89
	Sig.	0.000

5.5.3 Communalities

An increased share of common variance is indicated by a communality value that is close to one (Pallant, 2020). This indicates a relationship between the item and other items. On the other hand, an item with a low communality value or zero communality is thought to be distinct from other items (Pallant, 2020). It is crucial to remember that the suggested communality threshold should be higher than 0.30 (Pallant, 2020). Items with extraction values lower than 0.3 are, therefore, not connected to other items and it might be removed as invalid. It is important to note that communalities were evaluated for the given data and have a extraction value higher than 0.30 (see Table 5.6).

Table 5.6: Communalities Test

Communalities								
	Initial	Extraction		Initial	Extraction		Initial	Extraction
Q8_1	1,000	0,751	Q11_7	1,000	0,943	Q14_7	1,000	0,920
Q8_2	1,000	0,896	Q11_8	1,000	0,891	Q14_8	1,000	0,837
Q8_3	1,000	0,918	Q11_9	1,000	0,926	Q15_1	1,000	0,774
Q8_4	1,000	0,858	Q11_10	1,000	0,887	Q15_2	1,000	0,838
Q8_5	1,000	0,874	Q12_1	1,000	0,923	Q15_3	1,000	0,851
Q8_6	1,000	0,815	Q12_2	1,000	0,811	Q15_4	1,000	0,759
Q8_7	1,000	0,859	Q12_3	1,000	0,907	Q15_5	1,000	0,872
Q9_1	1,000	0,824	Q12_4	1,000	0,871	Q15_6	1,000	0,895
Q9_2	1,000	0,899	Q12_5	1,000	0,870	Q15_7	1,000	0,837
Q9_3	1,000	0,906	Q12_6	1,000	0,943	Q15_8	1,000	0,740
Q9_4	1,000	0,834	Q12_7	1,000	0,842	Q15_9	1,000	0,795
Q9_5	1,000	0,895	Q12_8	1,000	0,883	Q15_10	1,000	0,813
Q9_6	1,000	0,869	Q12_9	1,000	0,786	Q16_1	1,000	0,894
Q9_7	1,000	0,882	Q13_1	1,000	0,882	Q16_2	1,000	0,853
Q10_1	1,000	0,859	Q13_2	1,000	0,926	Q16_3	1,000	0,923
Q10_2	1,000	0,810	Q13_3	1,000	0,917	Q16_4	1,000	0,898
Q10_3	1,000	0,847	Q13_4	1,000	0,895	Q16_5	1,000	0,930
Q10_4	1,000	0,835	Q13_5	1,000	0,850	Q16_6	1,000	0,916
Q10_5	1,000	0,809	Q13_6	1,000	0,935	Q17_1	1,000	0,812
Q10_6	1,000	0,812	Q13_7	1,000	0,820	Q17_2	1,000	0,819
Q10_7	1,000	0,836	Q13_8	1,000	0,920	Q17_3	1,000	0,885
Q11_1	1,000	0,879	Q14_1	1,000	0,894	Q17_4	1,000	0,909
Q11_2	1,000	0,909	Q14_2	1,000	0,929	Q17_5	1,000	0,923
Q11_3	1,000	0,884	Q14_3	1,000	0,853	Q17_6	1,000	0,806
Q11_4	1,000	0,890	Q14_4	1,000	0,946	Q17_7	1,000	0,844
Q11_5	1,000	0,893	Q14_5	1,000	0,886			
Q11_6	1,000	0,898	Q14_6	1,000	0,915			

5.5.4 Total Variance Explained

The Total Variance Explained validity method loads factors in their categories to get an Eigenvalue greater than one. Factors with an Eigenvalue lower than one are irrelevant and the remaining elements or factors will be reliable (Pallant, 2020). Furthermore, the recommended cut-off point is a total variance explained of more than 60% for all valid components combined (Tredoux & Durrheim, 2013). The results of Total Variance explained on factors of this study was above 60%. Table 5.7 also shows the data of Total Variance explained on 18 factors. There were 86 components with an Eigenvalue greater than one after the initial analysis. The remaining 18 components consequently had an Eigenvalue greater than 2. The Kaiser criterion technique suggests that these two components be retained around for further analysis.

Table 5.7: Total Variance Explained

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	14,912	18,875	18,875	14,912	18,875	18,875
2	13,386	16,944	35,819	13,386	16,944	35,819
3	5,084	6,435	42,254	5,084	6,435	42,254
4	4,657	5,895	48,150	4,657	5,895	48,150
5	4,172	5,281	53,430	4,172	5,281	53,430
6	3,589	4,543	57,974	3,589	4,543	57,974
7	3,275	4,146	62,119	3,275	4,146	62,119
8	2,958	3,744	65,863	2,958	3,744	65,863
9	2,434	3,082	68,945	2,434	3,082	68,945
10	2,114	2,676	71,621	2,114	2,676	71,621
11	1,900	2,405	74,026	1,900	2,405	74,026
12	1,793	2,270	76,295	1,793	2,270	76,295
13	1,746	2,210	78,505	1,746	2,210	78,505
14	1,611	2,040	80,545	1,611	2,040	80,545
15	1,416	1,793	82,338	1,416	1,793	82,338
16	1,250	1,583	83,921	1,250	1,583	83,921
17	1,244	1,575	85,496	1,244	1,575	85,496
18	1,090	1,380	86,875	1,090	1,380	86,875
19	0,997	1,262	88,137			
20	0,928	1,175	89,312			
21	0,827	1,047	90,359			
22	0,799	1,011	91,370			
23	0,754	0,955	92,325			

24	0,692	0,876	93,201			
25	0,654	0,828	94,029			
26	0,607	0,769	94,798			
27	0,571	0,722	95,520			
28	0,488	0,618	96,138			
29	0,448	0,567	96,705			
30	0,415	0,525	97,229			
31	0,374	0,473	97,702			
32	0,301	0,381	98,083			
33	0,283	0,359	98,442			
34	0,261	0,330	98,772			
35	0,229	0,290	99,062			
36	0,172	0,218	99,280			
37	0,166	0,211	99,491			
38	0,131	0,166	99,657			
39	0,114	0,145	99,802			
40	0,084	0,106	99,908			
41	0,073	0,092	100,000			

5.5.5 Factor Rotated Component Matrix^a and Interpretation

The final validity test computed in this study was the rotated component matrix. The rotated component matrix generates groups of components or data sets and helps in the clarification of factor structure to provide clearly interpretable EFA test results (Luiten, Hox & de Leeuw, 2020). The test determines whether items from a particular factor load well or not. Loading was used to determine how well items were associated with their parent factor (Luiten et al., 2020). After factor loading, items that were not well grouped with their parent factor were deleted because they did not load well and could not represent the underlying factor (Luiten et al., 2020).

Table 5.8: Rotated Component Matrix

	Component																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Q8_1	0,558																	
Q8_2		0,746																
Q8_3		0,883																
Q8_4	0,776	0,237																
Q8_5	0,380	0,821																
Q8_6	0,808																	
Q8_7	0,673																	
Q9_1				0,573														
Q9_2			0,808															
Q9_3			0,821															
Q9_4				0,823														
Q9_5				0,810														
Q9_6			0,770															
Q9_7			0,759															
Q10_1						0,884												
Q10_2						0,849												
Q10_3						0,572												
Q10_4					0,883													
Q10_5					0,740													
Q10_6					0,766													
Q10_7					0,691													

Table 5.8: Rotated Component Matrix (continued)

	Component																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Q11_1							0,831											
Q11_2							0,692											
Q11_3									0,921									
Q11_4									0,733									
Q11_5								0,852										
Q11_6								0,672										
Q11_7								0,804										
Q11_8								0,822										
Q11_9								0,782										
Q11_10									0,774									
Q12_1										0,848								
Q12_2										0,562								
Q12_3										0,854								
Q12_4										0,659								
Q12_5										0,611								
Q12_6										0,808								
Q12_7											0,654							
Q12_8											0,684							
Q12_9											0,743							

Table 5.8: Rotated Component Matrix (continued)

	Component																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Q13_1												0,807						
Q13_2												0,850						
Q13_3												0,836						
Q13_4												0,827						
Q13_5											0,788							
Q13_6											0,901							
Q13_7											0,738							
Q13_8											0,904							
Q14_1												0,800						
Q14_2												0,918						
Q14_3												0,801						
Q13_5											0,788							
Q13_6											0,901							
Q13_7											0,738							
Q13_8											0,904							
Q14_1												0,800						
Q14_2												0,918						
Q14_3												0,801						
Q14_4												0,926						
Q14_5													0,785					
Q14_6													0,765					
Q14_7													0,724					
Q14_8													0,742					

Table 5.8: Rotated Component Matrix (continued)

	Component																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Q15_1														0,645				
Q15_2															0,851			
Q15_3															0,857			
Q15_4														0,802				
Q15_5														0,804				
Q15_6														0,873				
Q15_7															0,598			
Q15_8														0,795				
Q15_9																0,908		
Q15_10																0,605		
Q16_1					0,637													
Q16_2					0,781													
Q16_3					0,887													
Q16_4					0,887													
Q16_5					0,916													
Q16_6					0,909													
Q17_1																0,899		
Q17_2																0,844		
Q17_3																0,800		
Q17_4																0,145	0,881	
Q17_5																	0,917	
Q17_6																	0,801	
Q17_7																0,690		
Extraction Method: Principal Component Analysis. a. 18 components extracted.																		

In this study, a baseline of Pallant's (2020) finding of a 0.3 threshold was used to ensure that the retained items were suitable for further analysis. Items with values less than 0.3 were therefore removed in accordance with the suggested threshold (Luiten et al., 2020). On the other hand, items with a value of 0.5 or more after loading factors were retained because they showed that they loaded firmly on their underlying factors (Luiten et al., 2020).

Rotated Component Matrix was performed using the Varimax method with Kaiser Normalisation to check if factors could be independent. Varimax is the Orthogonal rotation, and it is the most common rotation method used in the Component matrix (Pallant, 2020). The Varimax rotation was appropriate for this analysis because it provides easier-to-understand factors, increasing the distribution of loading among factors (Pallant, 2020). The section below discusses the Rotated Component Matrix^a on factors.

Scree Plot

Figure 5.1 shows the Scree Plot graph on factors with an eigenvalue greater than one.

Figure 5. 7 Scree Plot

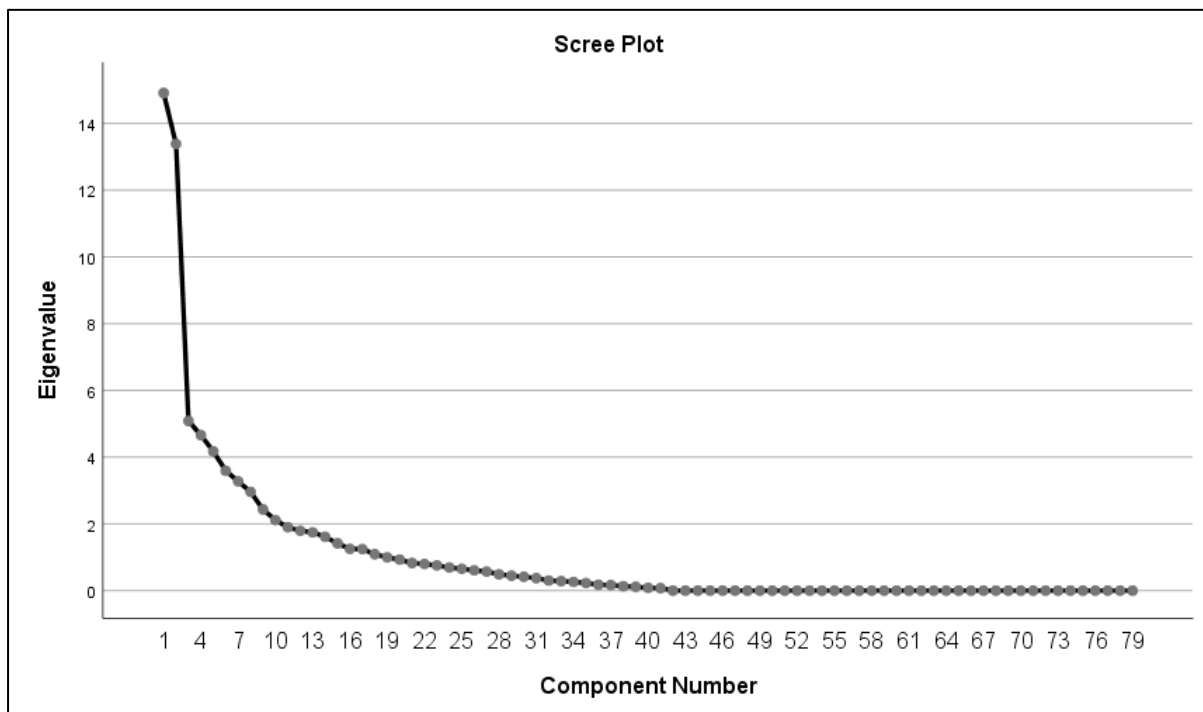


Figure 5.1 shows that 18 points fell just before the elbow bend when the curve slope flattens. These were the components with an Eigenvalue greater than one, as Pallant (2021) recommended. This meant that for further analysis, these 18 variables were kept. Furthermore, it suggested a relationship between 18 clusters of elements from the factors of Perceived Ease of Use in this situation. The 18 factors that were kept were subsequently subjected further to Varimax rotation analysis.

5.6 Reliability test (Cronbach Alpha)

Morgan, Barrett, Leech and Gloeckner (2019) define reliability as the degree to which the factor's measurement is trustworthy and consistent. For the factor to be reliable, the measuring equipment must produce the same results with no errors (Tredoux and Durrheim, 2013). This consistency should be obtained over various conditions and give the same results. The same meaningful results are provided during the reliability test under the exact measurements that are repeated using the same conditions and consistently (Gravetter & Wallnau, 2017). In research, reliability is the ability of the instrument to repeat and replicate research findings (Gravetter & Wallnau, 2017).

In the context of this study, reliability testing was used to ensure that the measuring instrument (questionnaire) was consistent throughout and reliable (Gravetter & Wallnau, 2017). Decision factors were evaluated for reliability before testing correlation and factor validity. Cronbach's Alpha was used to assess the internal consistency of these variables. Additionally, each item on the questionnaire was subjected to item analysis to determine the internal consistency of these decision variables. Internal consistency was reflected through the factor reliability of the scale items by measuring the same factor for the data collected (Huizingh, 2007). Furthermore, reliability was used to evaluate the correlation between items and a factor, and the scaling was determined by the Cronbach Alpha coefficient (α) (Heo, Kim & Faith, 2015). The reliability test was done in this study to find relationships between variables.

A Likert scale of 1 to 5 was used in the questionnaire for questions 8 to 17, with 1 being strongly agreed and 5 strongly disagree. The Cronbach Alpha was used to determine the factor reliability of the scale items. Furthermore, the value Cronbach Alpha was used to determine if the variables were internally dependable and the reliability of the questionnaire. All valid factors

were evaluated separately to measure the internal consistency of data items. The Cronbach Alpha value is the most widely used metric for assessing the internal consistency of item scales that demonstrates reliability, according to Stehlik-Barry & Babinec (2017). Furthermore, studies have shown that it is the most widely accepted reliability indicator, particularly when using the Likert scale (Pallant, 2020). Table 5.9 shows the calculations the researcher performed using the Cronbach Alpha to determine which items to include and exclude from the questionnaire (Heo, Kim & Faith, 2015).

Table 5.9: Cronbach's α Values Interpretation

Value of Cronbach Alpha	Interpretation
Less than 0.5	Unacceptable or poor
Greater than 0.50 and less than 0.69	Moderate reliable
Greater than 0.70 and less than 0.89	Good or highly reliable
above 0.9	Excellent

According to Tredoux & Durrheim (2013), when measuring Cronbach Alpha, on a scale from 0 to 1, anything greater than 0.7 is considered highly reliable. The Cronbach Alpha value was calculated in this study using SPSS (Statistical Package for the Social Sciences) version 25 to assess each factor's reliability.

Cronbach Alpha Results

The analysis of the factors demonstrated that all of them were highly dependable. It is worth noting that all the factors had Cronbach Alpha values that ranged from 0.689 to 0.936, indicating that the conclusions were highly dependable. The Cronbach Alpha results showed that all the factors and items established to test the effectiveness of cyber-security controls on DHIS to prevent cyber-attacks were highly reliable in this study. Hence all the factors were reliable with a Cronbach Alpha value of above or equal to 0.6. Tables 5.10 to 5.13 shows the values for Cronbach Alpha.

Table 5.10: Reliability Factor of Technology Threat Avoidance Theory

Item-Total Statistics Perceived Severity					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q8_1	10,12	10,858	0,271	0,764	0,744
Q8_2	10,17	10,316	0,404	0,728	
Q8_3	10,36	10,311	0,449	0,716	
Q8_4	10,43	10,519	0,570	0,695	
Q8_5	10,26	9,123	0,728	0,648	
Q8_6	10,36	10,023	0,508	0,702	
Q8_7	10,31	11,687	0,375	0,732	
Item-Total Statistics Perceived Susceptibility					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q9_1	11,76	11,607	0,610	0,801	0,828
Q9_2	12,24	12,807	0,633	0,795	
Q9_3	12,40	13,347	0,576	0,805	
Q9_4	12,50	14,268	0,375	0,834	
Q9_5	12,62	14,830	0,521	0,819	
Q9_6	11,74	12,099	0,660	0,789	
Q9_7	11,74	11,427	0,706	0,780	
Item-Total Statistics Combined Perceived Effectiveness (security software) and Perceived Effectiveness (controls)					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q10_1	20,48	25,931	0,593	0,902	0,906
Q10_2	20,67	26,864	0,635	0,898	
Q10_3	20,86	28,155	0,685	0,897	
Q10_4	20,95	29,086	0,473	0,904	
Q10_5	20,95	28,318	0,563	0,901	
Q10_6	20,74	28,035	0,638	0,898	
Q10_7	20,67	28,400	0,341	0,914	
Q16_1	20,81	27,995	0,515	0,903	
Q16_2	20,90	27,543	0,716	0,895	
Q16_3	20,74	27,027	0,704	0,895	
Q16_4	20,86	26,523	0,737	0,893	
Q16_5	20,67	25,856	0,842	0,888	
Q16_6	20,71	26,222	0,801	0,890	

Table 5.10 Reliability Factor of Technology Threat Avoidance Theory (Continued)

Item-Total Statistics Self-Efficacy					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q11_1	23,36	54,471	0,715	0,914	0,922
Q11_2	23,52	56,267	0,651	0,917	
Q11_3	23,17	57,356	0,558	0,922	
Q11_4	23,31	54,407	0,787	0,910	
Q11_5	23,64	54,615	0,800	0,910	
Q11_6	23,57	54,151	0,776	0,910	
Q11_7	24,07	55,219	0,724	0,913	
Q11_8	24,05	55,006	0,794	0,910	
Q11_9	23,50	54,396	0,730	0,913	
Q11_10	23,31	56,231	0,556	0,924	

Table 5.11: Technology, Organisation, Environment (TOE)

Item-Total Statistics (Training)					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q12_1	14,33	15,545	0,817	0,766	0.837
Q12_2	15,57	21,031	0,239	0,877	
Q12_3	14,57	15,226	0,844	0,759	
Q12_4	14,98	16,609	0,612	0,812	
Q12_5	15,02	18,170	0,589	0,815	
Q12_6	14,69	18,756	0,632	0,811	
Item-Total Statistics Top Management Support					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q13_1	19,10	32,055	0,741	0,929	0,936
Q13_2	19,14	31,371	0,800	0,925	
Q13_3	19,24	32,151	0,775	0,927	
Q13_4	19,26	32,691	0,769	0,928	
Q13_5	18,69	31,415	0,723	0,931	
Q13_6	18,95	29,950	0,867	0,920	
Q13_7	19,45	32,458	0,663	0,935	
Q13_8	19,33	30,464	0,867	0,920	

Table 5.12: Technology Acceptance Model

Item-Total Statistics Perceived Ease of Use					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q14_1	13,62	19,006	0,627	0,883	0,892
Q14_2	13,64	18,039	0,713	0,875	
Q14_3	13,60	16,947	0,851	0,861	
Q14_4	13,64	17,799	0,759	0,871	
Q14_5	13,17	18,140	0,538	0,892	
Q14_6	13,36	16,791	0,793	0,866	
Q14_7	13,50	17,388	0,824	0,865	
Q14_8	12,98	17,639	0,444	0,912	
Item-Total Statistics Usefulness					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q15_1	16,57	18,007	0,504	0,813	0,825
Q15_2	16,05	14,926	0,577	0,805	
Q15_3	15,88	16,282	0,430	0,823	
Q15_4	16,48	17,243	0,549	0,807	
Q15_5	16,57	17,095	0,739	0,796	
Q15_6	16,50	17,292	0,714	0,799	
Q15_7	16,12	14,698	0,618	0,799	
Q15_8	16,45	17,098	0,644	0,800	
Q15_9	16,19	17,531	0,300	0,835	
Q15_10	16,48	18,107	0,451	0,816	

Table 5.13: Threat Avoidance Theory (TTAT) Factors

Item-Total Statistics Cyber-Attack Avoidance					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Cronbach's Alpha
Q17_1	13,74	11,859	0,312	0,676	0,689
Q17_2	13,50	11,820	0,303	0,677	
Q17_3	13,52	11,243	0,393	0,658	
Q17_4	12,95	8,638	0,621	0,580	
Q17_5	12,62	8,638	0,476	0,638	
Q17_6	12,86	10,011	0,393	0,658	
Q17_7	13,52	12,107	0,343	0,673	

5.7 Descriptive statistics

Perceived Severity, Perceived Susceptibility, Perceived Effectiveness (Policy), Training, Top Management Support, Perceived Effectiveness (Software) and Cyber-Attack Avoidance Motivation were studied. N stands for the overall number of items across all factors. The minimum value was one, and the maximum value was five, as shown in descriptive Table 5.14. The maximum and minimum standard deviations were 0.44 and -0.83, respectively.

Table 5.14: Descriptive Statistics

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Q8: Perceived Severity	126	1,00	3,00	1,7143	0,52652
Q9: Perceived Susceptibility	126	1,00	3,29	2,0238	0,59047
Q10: Perceived Effectiveness (Policies)	126	1,00	2,71	1,7415	0,43395
Q11: Self-Efficacy	126	1,10	5,00	2,6167	0,82207
Q12: Training	126	1,22	3,56	2,6164	0,50491
Q13: Top Management	126	1,00	4,75	2,7351	0,79900
Q14: Perceived Ease of Use	126	1,00	3,88	1,9196	0,59675
Q15: Perceived Usefulness	126	1,00	2,90	1,8143	0,45144
Q16: Safeguard Effectiveness (Software)	126	1,00	3,33	1,7183	0,52216
Q17: Avoidance Motivation	126	1,00	3,29	2,2075	0,52949
Combine Q10 and Q16: SW Policies	126	1,00	2,81	1,7299	0,43781
Valid N (listwise)	126				

Descriptive analysis: Perceived Severity

The descriptive statistics for the Perceived Severity factor (Question 8) in Table 5.14 shows a mean = 1,71, which was rounded to 2. This mean showed that the respondents agreed on perceived severity. The sampled population agreed that a threat's perceived severity was a serious problem for them. The respondents agreed that the virus infection caused by opening a suspicious email attachment was a serious problem. They also agreed that violating the security policy could put them in trouble and that data loss due to hackers was a serious problem. Also, their work could be negatively affected by opening an email attachment with a virus infection. Ultimately, a data breach in the DHIS system could be a significant issue. Therefore, we concluded that the sampled population agreed that the perceived severity of a threat on DHIS is a severe problem for them.

Descriptive analysis: Perceived Susceptibility

Descriptive statistics on the Perceived Susceptibility factor (Question 9) showed a mean = 2,02 and SD = 0,6, as shown in Table 5.14. When rounded to the nearest whole number, the Mean = 2. This implies that the respondents agreed on the factor of perceived susceptibility. The perceived susceptibility factor evaluates the security damage that cyber-attacks on the DHIS could cause. The security damages to the DHIS could be due to opening a suspicious email attachment infected by a virus. Another risk could be losing patients' data saved on the DHIS due to hacking or a security breach. Daily work could be negatively affected when there is a cyber-attack. Again, violating security policies and procedures set to prevent cyber-attacks on DHIS.

Descriptive analysis: Perceived Effectiveness (policy)

The Perceived Effectiveness (policy) (Question 10) had an average mean of 1.72 and a standard deviation of 0.53. The mean was rounded off to a whole integer of 2. According to the results, most respondents agreed that security policies could help reduce cyber-attacks. Information security breaches can be minimised with the assistance of respondents who concurred with the statement "adhering to information security policies". Moreover, they concur that using security technology protects personal information. It can be urged that, if properly implemented, DHIS security measures could secure personal information.

Descriptive analysis: Self-Efficacy

As shown in Table 5.14, Self-Efficacy (Question 11): M = 2.62, SD= 0.83. Mean was rounded to M = 3. This indicated that respondents' feelings towards the Self-Efficacy set of questions were neutral. Similarly, their typical response was neutral when asked if their organisation regularly reminds them to follow internet and computer security policies. Answers were also neutral when asked about their confidence in using different security settings in web browsers, handling virus-infected files, and removing viruses or malware from their machines.

Participants were also asked about their knowledge of cyber-security-related terms, different programs that could safeguard the DHIS, and developing advanced skills to safeguard the DHIS. The majority of the responses did not agree or disagree with the statements made. This

is clearly seen in Figure 5.2. When participants were questioned about whether they could confidently use the user's guide when they needed assistance protecting DHIS, the results were neutral. Participants were also questioned on their ability to put security measures in place to block access to private data and on their ability to spot suspicious email attachments even in the absence of assistance.

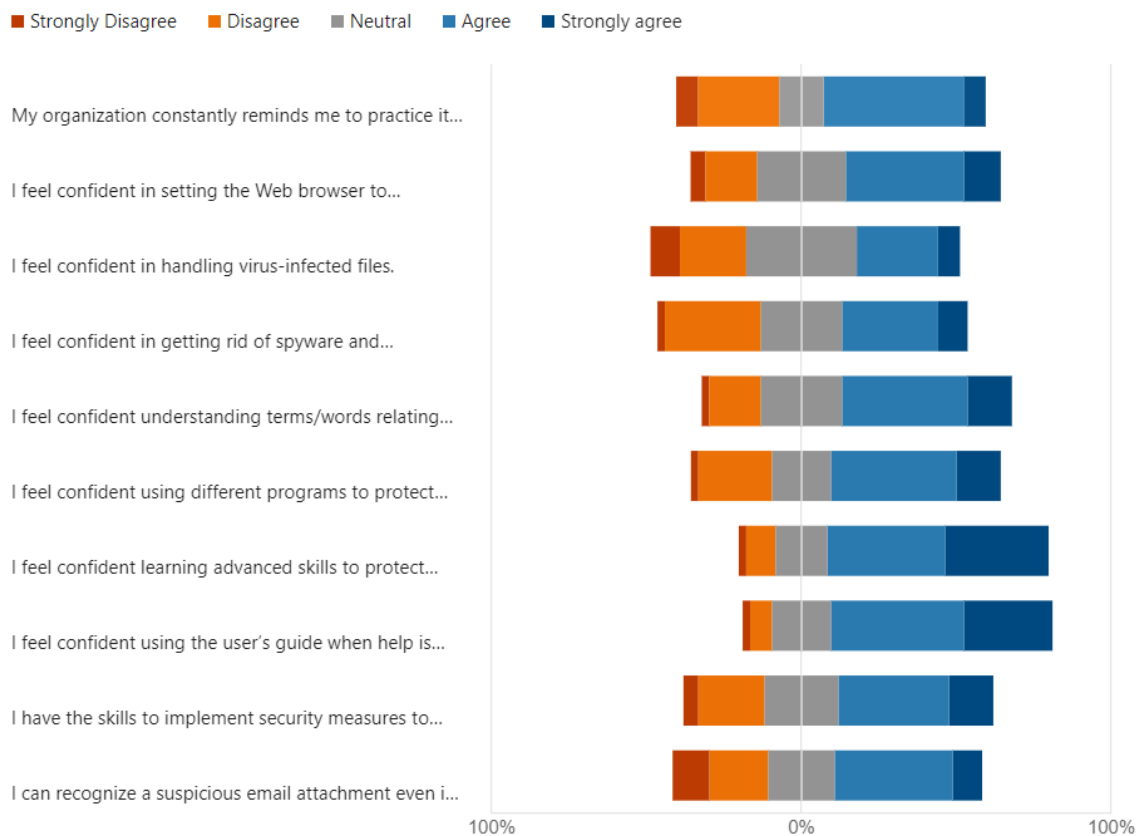


Figure 5. 8 Bar Chart of Responses Regarding Self-Efficacy

Descriptive analysis: Training

The researcher measured user satisfaction with the Training factor (Question 12). On average, the survey respondents got a mean of $M = 2.62$ and a standard deviation of $SD = 0.60$. The mean was rounded off to a whole integer of $M = 3$, representing that most DHIS users neither agreed nor disagreed that the organisation provided them with training in cyber-security awareness. Furthermore, the findings showed a neutral response from top management regarding providing support training to equip DHIS users with cyber-security skills. This is shown graphically in Figure 5.3.

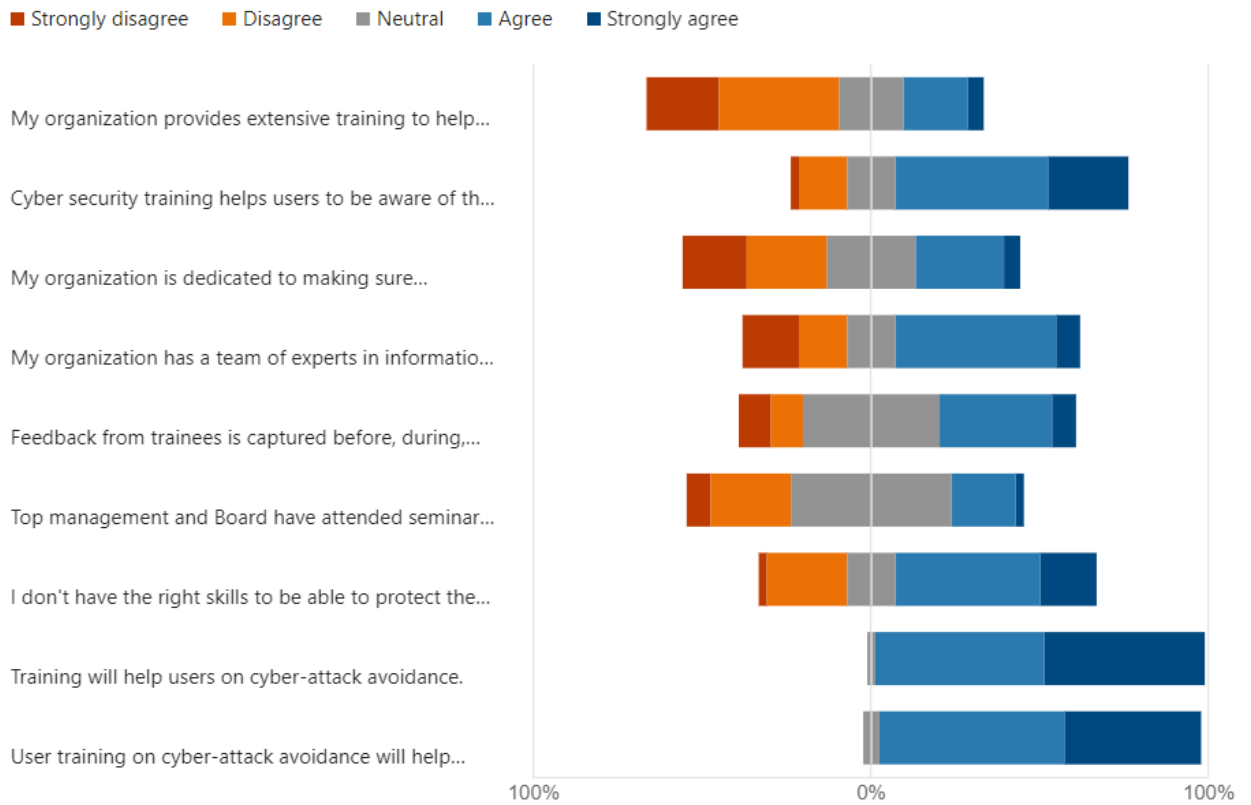


Figure 5. 9 Bar Chart of Responses for Training

Descriptive analysis: Top Management Support

Regarding the Top Management Support factor (Question 13), the overall feedback of respondents showed a mean of $M = 2.74$ and a standard deviation of $SD = 0.81$. The value of the mean was rounded off to the whole integer $M = 3$. The results showed that users neither agreed nor disagreed with whether top management supported cyber security measures for DHIS (see Figure 5.4). This includes investing in financial resources to prevent cyber-attacks as well as investing in information technology to ensure that DHIS is secured against cyber-attacks.

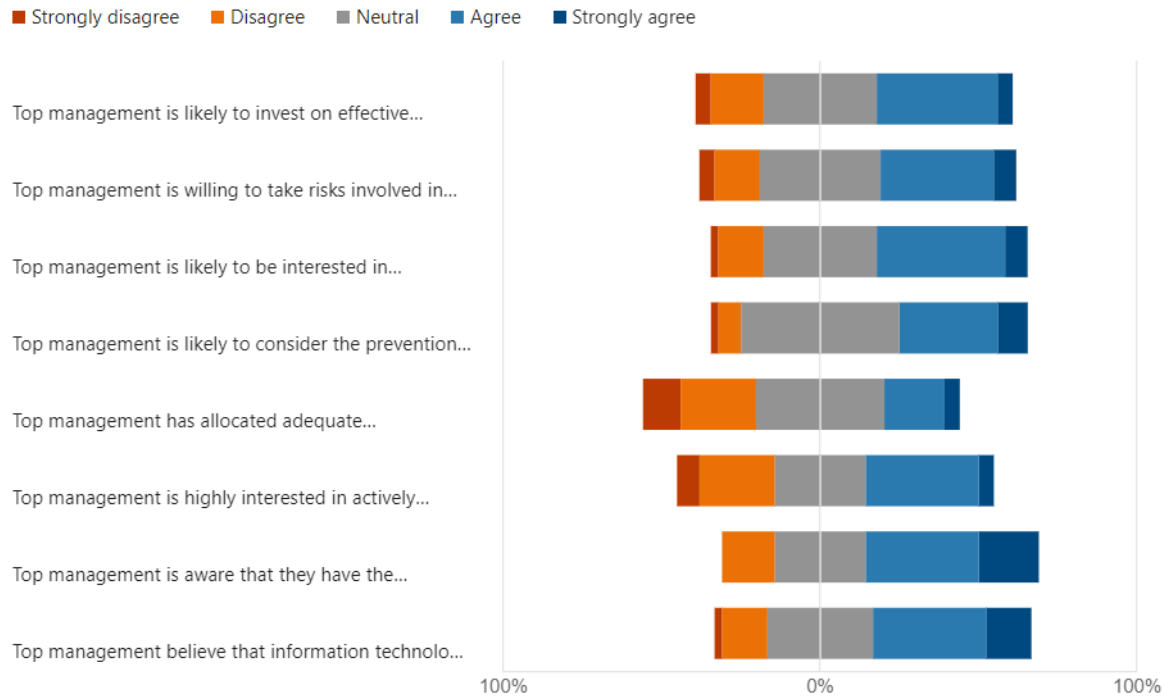


Figure 5. 10 Bar Chart of Responses Regarding Top Management Support

Descriptive analysis: Perceived Ease of Use

The Perceived Ease of Use factor (Question 14) had a mean of 1.92 and a standard deviation of 0.82, as indicated in Table 5.14. The value of the mean was rounded ($M = 2$), which showed that participants agreed with the items on the factors.

Descriptive analysis: Perceived Usefulness

The Mean of Perceived Usefulness (Question 15) was $M = 1.82$, and the standard deviation was $SD = 0.5$. The mean value was rounded off to the nearest whole integer of $M = 2$. This implied that respondents agreed that the DHIS system was useful to them. Respondents agreed that the DHIS system improves job efficiency and that patient data was secured. Respondents also agreed that the DHIS system would speed up the transfer of patient information and influence healthcare service delivery.

Descriptive analysis: Perceived Effectiveness (software)

The average mean (M) of the dependent variable Perceived Effectiveness (Software) (Question 16): $M = 1.74$; standard deviation of (SD) = 0.44. The M value was rounded to $M = 2$. This indicates that users agreed with the Perceived Effectiveness (software) question items. In this question, users were asked about cyber-security software's effectiveness in preventing cyber-attacks. Users agreed that security software such as antivirus would prevent cyber-attacks effectively.

Descriptive analysis: Cyber-attack Avoidance Motivation

The dependent variable cyber-attack avoidance motivation factor (Question 17) had (SD = 0.53; $M = 2,21$). The M value was rounded off to 2. This value indicated that users agreed with statements concerning utilising security software to avoid cyber-attacks and DHIS Systems. Other questions related to security measures that could prevent security breaches and how users apply and adhere to them. Based on the findings, users agreed to run software security such as antivirus and anti-spyware software to prevent cyber-attacks.

5.8 Correlation Analysis

Correlation analysis gives a numerical summary of the strength and direction of the linear relationship between two variables. The analysis computed explained if there was a reasonable statistically significant relationship between the factors. Table 5.15 shows the output of the Pearson correlation, and the results are explained below. Variables tested for correlation were: From TTAT - Perceived Severity, Perceived Susceptibility, Self-Efficacy, Perceived Effectiveness (software and controls separately and combined) and Cyber-Attack Avoidance Motivation,

From TOE - Training, Top Management Support,

From TAM - Perceived Ease of Use, Perceived Usefulness,

A Pearson's r value in the range 0.30 to 0.59 shows a moderate relationship, while values in the range 0.60 to 0,89 point to a strong relationship.

Table 5.15: Correlation Statistics

		Correlations										
		PSev	PSus	PESW	PEP	SE	T	TMS	PU	AM	PEOU	SW+P
Perceived Severity (PSev)	Pearson Correlation	1	.614 **	.480 **	.499 **	0,006	-0,032	-.235 **	0,102	0,119	-0,071	.534 **
	Sig. (2-tailed)		0,000	0,000	0,000	0,951	0,726	0,008	0,254	0,183	0,430	0,000
	N	126	126	126	126	126	126	126	126	126	126	126
Perceived Susceptibility (PSus)	Pearson Correlation	.614 **	1	.478 **	.619 **	0,174	-0,139	-0,057	.225 *	-0,002	0,170	.592 **
	Sig. (2-tailed)	0,000		0,000	0,000	0,052	0,120	0,523	0,011	0,984	0,058	0,000
	N	126	126	126	126	126	126	126	126	126	126	126
Perceived Effectiveness Software (PESW)	Pearson Correlation	.480 **	.478 **	1	.675 **	0,045	0,010	-0,167	.338 **	0,145	0,113	.931 **
	Sig. (2-tailed)	0,000	0,000		0,000	0,620	0,912	0,061	0,000	0,105	0,208	0,000
	N	126	126	126	126	126	126	126	126	126	126	126
Perceived Effectiveness Policies (PEP)	Pearson Correlation	.499 **	.619 **	.675 **	1	-0,038	-.260 **	-.255 **	.210 *	0,035	0,017	.898 **
	Sig. (2-tailed)	0,000	0,000	0,000		0,674	0,003	0,004	0,018	0,698	0,852	0,000
	N	126	126	126	126	126	126	126	126	126	126	126
Self-Efficacy (SE)	Pearson Correlation	0,006	0,174	0,045	-0,038	1	.465 **	.508 **	.189 *	.378 **	.559 **	0,008
	Sig. (2-tailed)	0,951	0,052	0,620	0,674		0,000	0,000	0,034	0,000	0,000	0,931
	N	126	126	126	126	126	126	126	126	126	126	126
Training (T)	Pearson Correlation	-0,032	-0,139	0,010	-.260 **	.465 **	1	.572 **	0,107	.351 **	.274 **	-0,123
	Sig. (2-tailed)	0,726	0,120	0,912	0,003	0,000		0,000	0,232	0,000	0,002	0,171
	N	126	126	126	126	126	126	126	126	126	126	126

Table 5.14: Correlation Statistics (continued)

Correlations (continued)												
		PSev	PSus	PESW	PEP	SE	T	TMS	PU	AM	PEOU	SW+P
Top Management Support (TMS)	Pearson Correlation	-.235 **	-0,057	-0,167	-.255 **	.508 **	.572 **	1	.179 *	.190 *	.458 **	-.226 *
	Sig. (2-tailed)	0,008	0,523	0,061	0,004	0,000	0,000		0,044	0,033	0,000	0,011
	N	126	126	126	126	126	126	126	126	126	126	126
Perceived Usefulness (PU)	Pearson Correlation	0,102	.225 *	.338 **	.210 *	.189 *	0,107	.179 *	1	.276 **	.396 **	.305 **
	Sig. (2-tailed)	0,254	0,011	0,000	0,018	0,034	0,232	0,044		0,002	0,000	0,001
	N	126	126	126	126	126	126	126	126	126	126	126
Avoidance Motivation (AM)	Pearson Correlation	0,119	-0,002	0,145	0,035	.378 **	.351 **	.190 *	.276 **	1	.489 **	0,104
	Sig. (2-tailed)	0,183	0,984	0,105	0,698	0,000	0,000	0,033	0,002		0,000	0,248
	N	126	126	126	126	126	126	126	126	126	126	126
Perceived Ease of Use (PEOU)	Pearson Correlation	-0,071	0,170	0,113	0,017	.559 **	.274 **	.458 **	.396 **	.489 **	1	0,076
	Sig. (2-tailed)	0,430	0,058	0,208	0,852	0,000	0,002	0,000	0,000	0,000		0,400
	N	126	126	126	126	126	126	126	126	126	126	126
SW Policies (SW+P)	Pearson Correlation	.534 **	.592 **	.931 **	.898 **	0,008	-0,123	-.226 *	.305 **	0,104	0,076	1
	Sig. (2-tailed)	0,000	0,000	0,000	0,000	0,931	0,171	0,011	0,001	0,248	0,400	
	N	126	126	126	126	126	126	126	126	126	126	126
**. Correlation is significant at the 0.01 level (2-tailed).												
*. Correlation is significant at the 0.05 level (2-tailed).												

TOE factors

Training and Top Management Support had a Pearson's r value of 0.572 ($p < 0.01$), showing a moderate to a strong relationship. The respondents did have information that the questions were related to TOE, and the questionnaire grouped them together.

TAM factors

Perceived Ease of Use, Perceived Usefulness had a Pearson's r value of 0.396 ($p < 0.01$), showing a moderate relationship. As noted above, respondents were told in the questionnaire that these factors belong to the same TAM theory.

TTAT factors

- a) Perceived Effectiveness (software) and Perceived Effectiveness (controls) separately had a Pearson's r value of 0.675 ($p < 0.01$), showing a strong relationship.
- b) Perceived Effectiveness (software) and the combined set of data (SW+C) had a Pearson's r value of 0.931 ($p < 0.01$), showing a very strong relationship.
- c) Perceived Effectiveness (controls) and the combined set of data (SW+C) had a Pearson's r value of 0.898 ($p < 0.01$), showing a very strong relationship.

This shows that the data collected from Q10 and Q16 can be combined as a single set of data.

- d) Perceived Severity and Perceived Susceptibility had a Pearson's r value of 0.614 ($p < 0.01$), showing a moderate relationship.
- e) Perceived Severity and Perceived Effectiveness (software and controls separately and combined) had Pearson's r values of 0.480, 0.499 and 0.534 (all $p < 0.01$), showing moderate relationships.
- f) Perceived Susceptibility and Perceived Effectiveness (software and controls separately and combined) had Pearson's r values of 0.478, 0.619 and 0.592 (all $p < 0.01$), showing moderate relationships.
- g) However, the fourth factor, Self-Efficacy, was surprising as there was no correlation with any other TTAT dependent factors.

Relationships between the independent factors of TTAT do not show the same strength regarding Self-Efficacy as the factors used from TOE and TAM.

Combining models

- a) Self-Efficacy related to both TOE factors (Training had a Pearson's r value of 0.465 ($p < 0.01$) and Top Management Support had a Pearson's r value of 0.508 ($p < 0.01$), showing a moderate relationship.
- b) Self-Efficacy related to both TAM factors (Perceived Ease of Use had a Pearson's r value of 0.189 ($p < 0.05$) and Perceived Usefulness had a Pearson's r value of 0.559 ($p < 0.01$), showing a moderate relationship.

Self-Efficacy has significant correlations with the factors selected from TOE and TAM. However, Perceived Effectiveness (controls only) and Perceived Ease of Use are also correlated with Training. This correlation between factors from different models shows that the models have interests in common and supports an argument that combining them into a single framework. As has been done in the study reported here, raises some interesting questions and hence is useful but must be done with care.

5.8.1 Correlations with Cyber-Attack Avoidance Motivation

The most interesting results from the correlation statistics in Table 5.15 relate to Cyber-Attack Avoidance Motivation as these relate to the hypotheses.

TTAT

Perceived Severity and Cyber-Attack Avoidance Motivation had a Pearson's r value of 0.119 which is not statistically significant.

Perceived Susceptibility and Cyber-Attack Avoidance **Motivation** had a Pearson's r value of -0.002 which is not statistically significant.

Perceived Effectiveness (software and controls separately and combined) and Cyber-Attack Avoidance Motivation had a Pearson's r value of 0.104 which is not statistically significant.

However, Self-Efficacy and Cyber-Attack Avoidance Motivation had a Pearson's r value of 0.378 ($p < 0.01$) showing a moderate relationship.

TOE

Training and Avoidance Motivation had a Pearson's r value of 0.351 ($p < 0.01$), showing a moderate relationship.

Top Management Support and Avoidance Motivation had a Pearson's r value of 0.190 ($p < 0.05$), showing a weak relationship.

TAM

Perceived Ease of Use and Avoidance Motivation had a Pearson's r value of 0.276 ($p < 0.01$), showing a moderate relationship.

Perceived Usefulness and Avoidance Motivation had a Pearson's r value of 0.489 ($p < 0.01$), showing a moderate relationship.

5.8.2 Hypothesis testing based on correlations

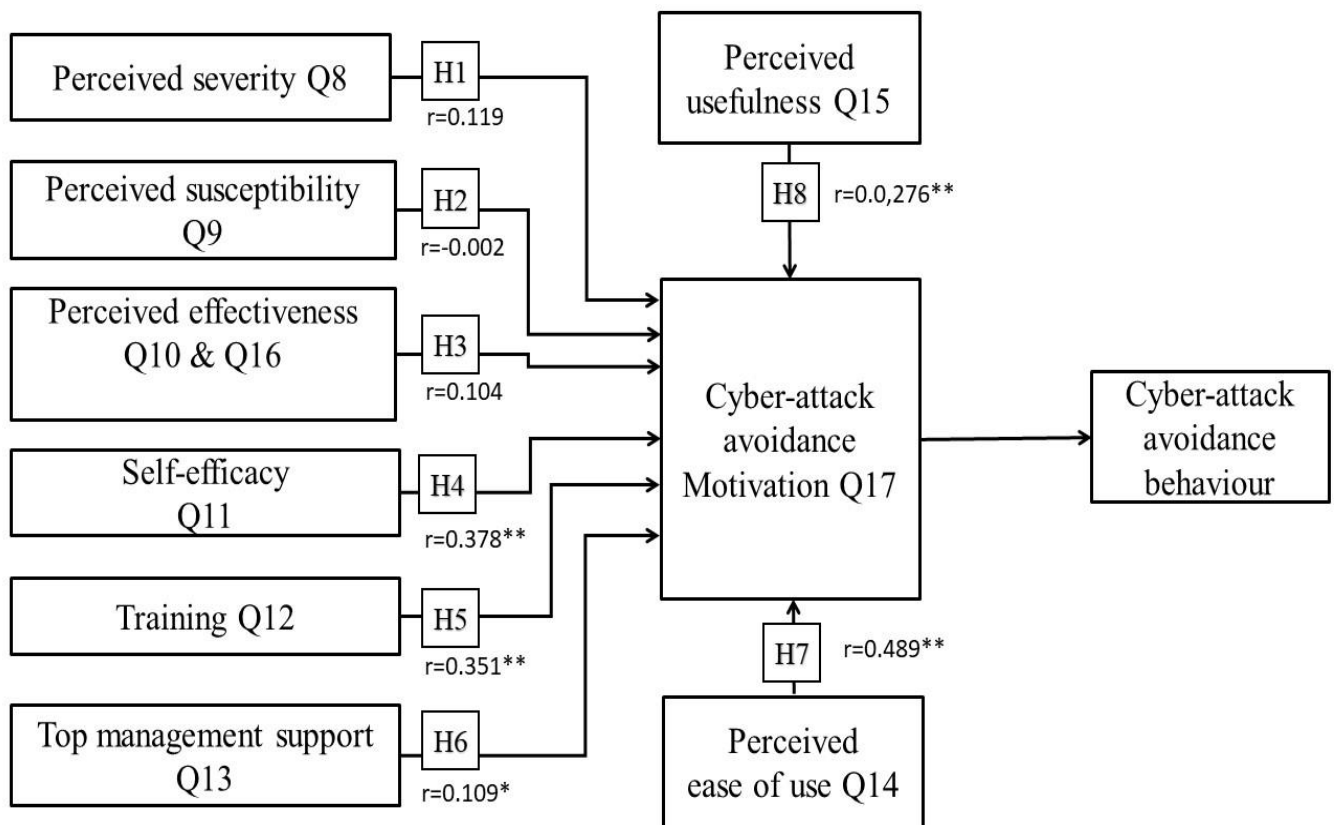


Figure 5. 11 Conceptual Framework with Correlation

Figure 5.2 shows r values obtained from Table 5.15, with * as being significant at $p < 0.05$ and ** as being significant at $p < 0.01$.

Table 5.16: Hypothesis Testing using Correlation

Hypotheses	Paths			r	P	Recommendation
H1	Cyber-attack Avoidance Motivation	←	Perceived Severity	0.119		Not supported
H2	Cyber-attack Avoidance Motivation	←	Perceived Susceptibility	-0.002		Not supported
H3	Cyber-attack Avoidance Motivation	←	Perceived Effectiveness	0,104		Not supported
H4	Cyber-attack Avoidance Motivation	←	Self-efficacy	0.378	<0.01	Supported
H5	Cyber-attack Avoidance Motivation	←	Training	0.351	<0.01	Supported
H6	Cyber-attack Avoidance Motivation	←	Top management	0.190	<0.05	Supported
H7	Cyber-attack Avoidance Motivation	←	Perceived Ease of Use	0,489	<0.01	Supported
H8	Cyber-attack Avoidance Motivation	←	Perceived Ease of Use	0.276	<0.01	Supported

5.9 Regression Analysis

Regression analysis refers to methods for modelling and analysing numerical data that consist of the value of independent and dependent variables (Huizingh, 2007). Huizingh (2017) further explained that regression analysis (usually known as modelling causal relationships) is a technique for testing hypotheses. Testing regression analysis is reliant firmly on underlying assumptions being met. In the context of this study, Multiple regression analysis was used to model the relationship between one continuous independent variable and other continuous dependent variables. Furthermore, the assumptions adopted for the study are listed below:

- No multicollinearity assumptions
- Autocorrelation of residuals assumptions
- Normality of residuals assumptions,
- Linearity assumptions
- Homoscedasticity assumptions.

5.9.1 Model Summary

The model summary in Table 5.17 provides an overview of the results. The dependent variable in the regression test in Cyber-attack Avoidance Motivation, while the independent variables were Perceived Ease of Use, Training and Top Management Support. Pearson's R-value represents the correlation between independent and dependent variables. The R in Table 5.17 had a value of 0.569. As a result, R reported a satisfactory level of correlation prediction of 57%, which was higher than the suggested threshold of 40%. This indicated that the Cyber-attack Avoidance Motivation factor had a 57% correlation with the Perceived Ease of Use, Training and Top Management Support factors. Hence the remaining potential contributing factors (Perceived Severity, Perceived Susceptibility, Perceived Effectiveness, Self-efficacy and Perceived Usefulness were excluded).

Table 5.17: Model Summary

Model Summary ^d										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin - Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.489 ^a	0,239	0,233	0,46385	0,239	38,880	1	124	0,000	
2	.538 ^b	0,290	0,278	0,44982	0,051	8,855	1	123	0,004	
3	.569 ^c	0,323	0,307	0,44085	0,034	6,058	1	122	0,015	2,433
a. Predictors: (Constant), Perceived Ease of Use										
b. Predictors: (Constant), Perceived Ease of Use, Training										
c. Predictors: (Constant), Perceived Ease of Use, Training, Top Management Support										
d. Dependent Variable: Avoidance Motivation										

Adjusted R-square represents the dependent variable's total variation explained by the independent variables. The adjusted R square means that the contribution of independent variables (Perceived Ease of Use, Training and Top Management Support), as illustrated in Table 5.17, had contributed 32% towards the Cyber-attack Avoidance Motivation factor. The adjusted R square had a value of 0.307, which was *not* higher than the suggested threshold. A

model should have a value greater than 0.5 to represent the effectiveness in determining the relationship between dependent and independent variables. For a model to be valid, the sig F change value must be less than 0.05. The significant F change value in the model summary table was 0.015, less than 0.05, indicating that the model was valid. As a result, the model summary interpreted data that met the requirements for the next phase in regression analysis: Analysis of Variance (ANOVA). The Adjusted R Square value indicated the Explanatory Power of the model (Battacherjee, 2012: 29).

5.9.2 ANOVA

Analysis of Variance evaluates whether the model is significant enough to determine the outcome (Tredoux & Durrheim, 2013). The Analysis of Variance preferred for this study was model three because the significant value for that model was less than 0.05. The overall multiple regression model was significant at a 95% confidence level with a p-value less than 0.05. F-ratio in the ANOVA tests if the overall regression model was suitable for the data. Because the value of p was less than the recommended threshold, Table 5.18 showed that the independent factors significantly statistically predicted the dependent variable, $F(3, 122) = 15.907$ ($p < 0.05$) (Tredoux and Durrheim, 2013). Therefore, the model had a statistically significant multilinear relationship between Perceived Effectiveness (software) and protection motivation and technology acceptance and threat avoidance factors.

Table 5.18: ANOVA

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8,365	1	8,365	38,880	.000 ^b
	Residual	26,680	124	0,215		
	Total	35,045	125			
2	Regression	10,157	2	5,079	25,099	.000 ^c
	Residual	24,888	123	0,202		
	Total	35,045	125			
3	Regression	11,335	3	3,778	19,440	.000 ^d
	Residual	23,711	122	0,194		
	Total	35,045	125			
a. Dependent Variable: Avoidance Motivation						
b. Predictors: (Constant), Perceived Ease of Use						
c. Predictors: (Constant), Perceived Ease of Use, Training						
d. Predictors: (Constant), Perceived Ease of Use, Training, Top Management Support						

5.9.3 Regression Coefficients of the factors

Table 5.19 shows the coefficient results, which indicate the variables' total contribution toward the equation or model. Again, model three was also chosen for Coefficients with variables Perceived Ease of Use, Training and Top Management Support. When looking closely at Table 5.19, these three variables had a statistically significant p-value of less than 0.05, as stated in the sig column. The standardised coefficient column in Table 5.19 shows the β value, which tells the amount each variable contributed to the equation or model.

Table 5.19: Coefficients

Coefficients ^a										
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	1,375	0,140		9,844	0,000	1,099	1,652		
	Perceived Ease of Use	0,434	0,070	0,489	6,235	0,000	0,296	0,571	1,000	1,000
2	(Constant)	0,840	0,225		3,730	0,000	0,394	1,286		
	Perceived Ease of Use	0,376	0,070	0,424	5,368	0,000	0,238	0,515	0,925	1,081
	Training	0,247	0,083	0,235	2,976	0,004	0,083	0,411	0,925	1,081
3	(Constant)	0,824	0,221		3,730	0,000	0,387	1,261		
	Perceived Ease of Use	0,446	0,074	0,503	6,002	0,000	0,299	0,593	0,790	1,265
	Training	0,369	0,095	0,352	3,875	0,000	0,181	0,558	0,672	1,488
	Top Management Support	-0,160	0,065	-0,242	-2,461	0,015	-0,289	-0,031	0,575	1,740

a. Dependent Variable: Avoidance Motivation

As a result of the findings described above, it was argued that certain motivating strategies in the DHIS environment effectively motivate the avoidance of cyber-attacks. An inspection of the individual predictors of the overall model revealed that Perceived Ease of Use ($\beta = 0,503$, $p < 0.05$), Training ($\beta = 0.352$, $p < 0.05$), Top Management Support ($\beta = -0.242$, $p < 0.05$) were

significant predictors of Cyber-attack Avoidance Motivation. Table 5.19 shows the results. All variables (Perceived Ease of Use, Training and Top Management Support) contributed statistically significant sig value of less than 0.05.

5.9.4 Hypotheses Testing

Following the model fit, the various relationships between variables were examined. Table 5.20 illustrates the correlation analyses' standardised significant values. The levels evaluate the relationship between the hypotheses and the structure of evaluating cyber-security controls efficacy. A hypothesis must have a Beta value of less than 0.5 to be accepted or the hypothesis will be rejected. The results are shown in Table 5.20. H5, H6, and H7 were statistically significant because their significant values were all more than 0.5. Together these three independent variables explain 31% of the model. The remaining 5 factors (Perceived Severity, Perceived Susceptibility, Perceived Effectiveness, Self-efficacy, and Perceived Usefulness) together could contribute a maximum of 100% - 31%, that is 69% between them but might add very little (see also Section 5.10). Looking closely at the significant values H5 ($\beta = 0.352$, $p < 0.05$), H6 ($\beta = -0.242$, $p < 0.05$) H7 ($\beta = 0.503$, $p < 0.05$), were their values. On the other hand, H1, H2, H3, H4, and H8 were rejected.

Table 5.20: Hypothesis Evaluation

Hypotheses	Paths			Beta	Recommendation
H1	Cyber-attack Avoidance Motivation	←	Perceived Severity		Not Supported
H2	Cyber-attack Avoidance Motivation	←	Perceived Susceptibility		Not Supported
H3	Cyber-attack Avoidance Motivation	←	Perceived Effectiveness		Not Supported
H4	Cyber-attack Avoidance Motivation	←	Self-efficacy		Not Supported
H5	Cyber-attack Avoidance Motivation	←	Training	0.352	Supported
H6	Cyber-attack Avoidance Motivation	←	Top management	-0.242	Supported
H7	Cyber-attack Avoidance Motivation	←	Perceived Ease of Use	0.503	Supported
H8	Cyber-attack Avoidance Motivation	←	Perceived Usefulness		Not Supported

5.10 Discussion

According to Bhattacharjee (2012), a good theory is expected to:

- **Logical consistency: Does the theory** make logical sense? Can it be explained, and will others consider it to be rational?
- **Explanatory power:** When empirical research is done on the basis of the theory, the statistical analysis reports to what extent the theory explains the data. This is the Explanatory power which can be measured by the variance explained (R-square) value in regression equations.
- **Falsifiability:** Can the theory be disproved? This is applicable to empirical research and easier to show when a positivist research approach has been followed as it requires empirical data that clearly does not support the propositions of the theory.
- **Parsimony:** This is evident if a small number of variables explain the results well. “Parsimony examines how much of a phenomenon is explained with how few variables” (Battacharjee, 2012:29).

The second and the fourth of these characteristics are relevant as a basis for addressing the question regarding why the results given from the correlation analysis (Section 5.8) and those given from the regression analysis (Section 5.9) seem contradictory. The correlation analysis supported the acceptance of 5 hypotheses (H4, H5, H6, H7, H8), while the regression analysis only supported H5, H6 and H7. It is noticeable that the 3 question sets where the descriptive analyses show a more mixed response from the research participants, namely Self-Efficacy (H4), Training (H5), and Top Management Support (H6), all feature in the lists of supported hypotheses. These were only 3 sets of questions where the respondents did not overwhelmingly agree with the questions posed. Training was one of these (Top Management Support and Self-Efficacy were the two others). This more mixed response was in clear contrast with the overwhelming agreement with the other sets of questions and seemed to indicate that respondents might have engaged more actively with these questions as they had greater personal experience of them than other sets of questions (such as Perceived Severity and Perceived Susceptibility) that might have been based on reports in the press only.

Only the regression analysis provides an R-square value for this study that was 32,3% for model 3. This is where 3 independent variables were retained, which is not high. The remaining

independent variables did not add sufficiently to the explanatory power and hence, in the interests of parsimony, were excluded from the model.

The correlation analysis retains all the independent variables and supports H4 and H8. It might seem that correlation was 'better'. However, it can be argued that the independent variable Perceived Effectiveness (of both security controls and security software) used in H3 and that the independent variable Perceived Usefulness used in H8 overlapped considerably with other variables. For example, was the usefulness of the DHIS (Perceived Usefulness) really related to Perceived Severity, as the loss of the DHIS would be covered by several of the questions in the questionnaire under Perceived Severity? If this is accepted, H1 and H8 overlap.

Similarly, the Self-Efficacy variable used in H4 could possibly be related to Perceived Ease of Use in H7 even though the questions in the questionnaire clearly and consistently use the Perceived Ease of Use questions to ask about the DHIS and the Self-efficacy questions relate to the ability to apply security controls and security software. If this is accepted, H4 and H7 overlap.

H1, H2 and H3 were rejected both in the correlation and the regression analyses. Suppose it is assumed that H1 is covered to some extent (though not entirely) by H8. In that case, it leaves the interesting questions as to why cyber-attack avoidance motivation is not increased by a) Perceived Susceptibility (vulnerability of the HIS to cyber-attacks) and b) Perceived Effectiveness (the belief that the problem of cyber-attacks can be minimised or even eliminated if the existing policies, procedures and software are used properly as these are all effective).

Did the inclusion of overlapping concepts as though they were separate mean that potentially valuable insights became buried?

The correlation analysis shows significant relationships between pairs consisting of independent and dependent variables without considering whether there are overlaps between independent variables. The regression analysis shows significant relationships between pairs consisting of an independent variable and a dependent variable only if these make an additional contribution to the explanatory power of the model.

It is important to note that rejected hypotheses have not been proven to be false. Rather, there is insufficient evidence to show that they are true.

5.11 Conclusion

In this chapter, the study's quantitative data analysis was discussed. Effectiveness of DHIS cyber-security controls in preventing cyber-attacks at Tshwane district healthcare centres was also investigated in this chapter. As is usual when questionnaires are used, the respondents agreed unambiguously with most of the sets of questions. The questions were all presented as positive statements. Very nearly all the respondents agreed fully with questions regarding: Perceived Severity, Perceived Susceptibility, Perceived Effectiveness (security policy and controls), Perceived Effectiveness (security software), Top Management Support, Perceived Ease of Use, Perceived Usefulness

In addition, the respondents declared that they would use the security software provided and abide by security measures. This is in contrast with the response to the question regarding how often they change their passwords (Question 6). A 57% admitted it was 'sometimes', 'rarely' or 'never'. This supports the view above that respondents generally give answers that reflect well on them or that they think the researcher will think is 'correct'.

There were more mixed opinions about Training, Self-Efficacy and Top Management Support. Many respondents took a neutral stance on these questions, but several actively disagreed. Responses to other security-related information systems knowledge regarding anti-virus software and firewall protection on work computers 'no' or 'don't know' in between 40% and 50% of the cases which was in line with the responses regarding Training, Self-Efficacy. The data was analysed using correlations and multilinear regression to offer quantitative evidence of the effectiveness of cyber-security procedures. The hypotheses were tested and either accepted or rejected based on their significance value.

The results from the correlation analysis and multilinear regression analysis were compared and interrogated. Taking into account the importance of a theory which does not include redundant elements, the acceptance of only three hypotheses from the 8 proposed is an acceptable result. The following hypotheses were accepted:

H5: Increased levels of Training has an increased positive impact on Cyber-attack Avoidance Motivation.

H6: Increased Top Management Support has an increased positive impact on Cyber-attack Avoidance Motivation.

H7: Increased levels of Perceived Ease of Use has an increased positive impact on Cyber-attack Avoidance Motivation.

It is noticeable that Training and Top Management Support both were selected from TOE and Perceived Ease of Use comes from TAM. These are both very well-established theories. None of the factors from TTAT had proven significant relationships with Cyber-attack Avoidance Motivation.

The following were rejected:

H1: Increased Perceived Severity has an increased positive impact on Cyber-attack Avoidance Motivation.

H2: Increased Perceived Susceptibility has an increased positive impact on Cyber-attack Avoidance Motivation.

H3: Increased Perceived Effectiveness has an increased positive impact on Cyber-attack Avoidance Motivation.

H4: Increased Self-efficacy has an increased positive impact on Cyber-attack Avoidance Motivation.

H8: Increased levels of Perceived Usefulness has an increased positive impact on Cyber-attack Avoidance Motivation.

CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

6.1 Research Overview

This research aimed to investigate ways for cyber-attacks avoidance by increasing the effectiveness of cyber-security controls on the DHIS at Tshwane District Healthcare Centres. The underlying assumption made in this research was that cyber-security controls in the DHIS will only become fully effective as a means to prevent cyber-threats in healthcare centres if the people interacting with the DHIS are motivated to adhere to those controls and then consistently act in accordance with the prescribed processes and procedures.

The theoretical basis for the research comes from a combination of theories and frameworks. Some but not all of the factors come from two of the most well-known frameworks guiding research on technology acceptance (TAM), and contextual ways to analyse the organisational adoption⁵ of an information system (TOE) were included. Not all of the factors in TAM and TOE were used. Other factors were taken from TTAT, a more recent and more focused theory that is intended specifically for technology use in the context of Information Technology security. It is acknowledged that TTAT is based largely on Protection Motivation Theory.

A conceptual framework was developed to achieve the research purpose using related hypotheses. Empirical research data were collected and quantitatively examined using SSPS version 26.

6.2 Addressing the research problem

The aim of the research was to fill a research gap by investigating the factors that might influence the effective use of cyber-security controls in a state-managed environment (DHIS at Tshwane district healthcare centres). The assumption was made that these factors achieved the goal by encouraging (motivating) users to accept existing security policies, control measures and security software. The study was evaluated utilising the TAM, TTAT and TOE

⁵ Note that the term organization adoption refers to the decision taken by the designated decision maker to acquire the technology and to create policies and processes to allow, encourage and even require its use within the organization.

lenses. The eight hypotheses were developed based on the conceptual framework to answer the research objectives and will be discussed below. Data were collected from 126 participants using the online survey method. It was then statistically analysed using a quantitative approach and SPSS Version 26 as a tool.

It is important to note that evidence of actual cyber-attack avoidance behaviour (data) was not collected.

6.3 Addressing the research objectives and hypotheses

Research objective 1: To determine what cyber-attacks are common in the healthcare sector.

Research objective 2: To assess what damage such attacks may cause at healthcare centres.

These first two research objectives were partially answered in the literature review (Chapter 2 section 2.3 and section 2.4).

Research objective 3: To improve cyber-security of the DHIS by determining the current levels of knowledge of cyber-security policy, processes, and software by the users of the DHIS system and to what extent the respondents reported that they intend to carry out the required controls.

This objective was addressed using data collected from the questionnaire. Descriptive statistics were used (see Section 5.4). The participants were asked if a firewall was enabled on their computers. About half (52.30%) of respondents believed that was the case and they were protected to some extent against cyber-attacks. 64% of participants said they knew about the organisation's security policies. Anti-virus software knowledge was 69% knew it was installed; fewer (55%) knew whether it was actually active; and about the same number (52%) knew whether it was regularly updated. These seem to be realistic numbers. The installation, activation and updating of security software is not the responsibility of the lower-level data capturers, who made up the largest part (74%) of the research group. They do not even need to be aware of it.

Research objective 4: To improve cyber-security of the DHIS by determining what would motivate the users of the DHIS system to adhere more fully to cyber-security policy, processes and the use of software intended to detect and prevent breaches of the DHIS system.

This last research objective was answered by the data analysis and interpretation of the empirical research related to the hypotheses that follow.

H1: *Increased Perceived Severity has an increased positive impact on Cyber-attack Avoidance Motivation.*

It was proposed that the perceived level of cyber-attack severity on DHIS would positively impact Cyber-attack Avoidance Motivation. The hypothesis testing, however, did not find that perceived severity has a positive impact on motivation to avoid cyber-attacks by adhering to the organisation's security policies or control measures. Therefore, hypothesis one was not supported.

This is in line with the findings of some other studies (Ng, Kankanhalli & Xu, 2009. (Boon-Yuen et al., 2009; Zhang & McDowell, 2009). In contrast, a study by Ehizibue (2022) showed that perceived severity was a statistically significant factor. The findings supported the author's claim in his research that perceptions of phishing attack severity have a positive influence on behaviour to prevent attacks. The significance of perceived severity in achieving improved compliance with technology threat avoidance was further demonstrated by other studies (Chenoweth et al., 2009; Mohamed & Ahmad, 2012).

The descriptive statistics on perceived severity (see Table 5.14) showed that participants agree that cyber-attacks could pose a severe security threat to DHIS. Therefore, we conclude that the sampled population agreed that the perceived severity of a threat on DHIS was a severe problem for them, but the data analysis could not show this as being significantly related to cyber-attack avoidance motivation. While the importance of the perceived threat severity was high to participants, it is imperative to note that the impact or consequence of such an incident would only become real to the users should that incident, in fact, occur. Some authors think that awareness of the severity of the threat cannot be taken for granted – it is necessary to constantly alert people to current threats (Ahmed et al., 2017).

H2: *Increased Perceived Susceptibility has an increased positive impact on Cyber-attack Avoidance Motivation.*

The perceived likelihood of a cyber-incident occurrence was measured by the Perceived Susceptibility factor, but in this study, hypothesis 4 could not be shown to be true. It could not be shown that respondents would have increased motivation to take measures to avoid a potential cyber-attack even if they thought it was very easy for a cyber-criminal to breach the DHIS. This does not agree with studies done by Mohamed and Ahmad (2012) found that Perceived Susceptibility has a positive impact on achieving improved compliance with technology threat avoidance.

H3: *Increased Perceived Effectiveness has an increased positive impact on Cyber-attack Avoidance Motivation.*

Perceived Effectiveness is a measure of the respondent's belief that the two ways of protecting the DHIS from cyber-attacks, namely adherence to the security policies and security measures as well as the constant use of the security software, could effectively protect the DHIS. Hence, the respondents consider these policies, control measures and software reliability. The descriptive statistics on Perceived Effectiveness (policy) (see Section 5.7.3) and the descriptive statistics on Perceived Effectiveness (software) (see Section 5.7.9) both showed that participants agree that each of these are likely to be effective. In addition, as shown by the Cronbach Alpha test in Section 5.6.1, it was acceptable to combine the data from the two sets of questions creating a single data set for the variable Perceived Effectiveness.

The hypothesis testing results rejected the assumption that positive perceptions of effectiveness motivate users to adhere to cyber-attack avoidance security policies and security measures as well as the constant use of the security software. The results mean that even if respondents believe that the prevention policies and practices established by the organisation would be effective (which the descriptive analysis shows is the case), it could not be shown that this increases motivation to avoid potential attacks.

Studies that supported the Response Efficacy factor (which is very similar to Perceived Effectiveness but comes from Protection Motivation Theory) have been done by Ng, et al. (2009), Woon, Tan and Low., (2005), Workman, Bonner and Straub, (2008), and Chenoweth

et al., (2009). These reported results are consistent with Bandura's (1982, p. 140) proposition that "in any given instance, the behaviour would be best predicted by considering both self-efficacy and outcome beliefs", where Perceived Effectiveness reflects outcome beliefs. However, one study failed to support that Response Efficacy has a positive impact in achieving improved compliance with technology threat avoidance (Mohamed & Ahmad, 2012).

H4: Increased Self-efficacy has an increased positive impact on Cyber-attack Avoidance Motivation.

The descriptive statistics for this factor given in Section 5.7.4 and Figure 5.2 show that not all users have confidence in their ability to use computers to maintain the effectiveness of DHIS. This relates to users' confidence in using computer software such as antivirus to safeguard the DHIS. Furthermore, the hypothesis testing results failed to support that Self-Efficacy positively impacts the motivation of users to adhere to cyber-attack avoidance measures. However, the correlation analysis did show a positive significant relationship between Self-Efficacy and Cyber-attack Avoidance Motivation. Suggestions as to why the correlation analysis and regression analysis may appear to disagree are put forward in the discussion in Section 5.10.

This study was not the only one which failed to support this hypothesis (H4) (Larose & Rifon, 2007; Youn, 2009). In contrast, studies that supported Self-Efficacy as being a significant factor in compliance with technology threat avoidance were done by Mohamed and Ahmad (2012) and Sylvester (2022). Caldwell (2013) has highlighted this - healthcare sectors lack IT skilled personnel in numbers.

H5: Increased levels of Training has an increased positive impact on Cyber-attack Avoidance Motivation.

As noted in the discussion in Section 5.10, a noticeable number of respondents did not agree with or were neutral about the provision and importance of cyber-security training. Section 5.10 suggests that this reflects a considered response by the people completing the questionnaire. Section 5.7.5 and Figure 5.3 present the descriptive statistics for the set of questions regarding training. Table 5.16 shows that the correlation analysis found a significant relationship between training and the motivation of users to adhere to cyber-attack avoidance measures. Table 5.20 shows that the multiple regression analysis found a significant

relationship between training and the motivation of users to adhere to cyber-attack avoidance measures. This is highlighted in the literature - healthcare sectors lack IT-skilled personnel in numbers (Caldwell, 2013).

H6. Increased Top Management Support has an increased positive impact on Cyber-attack Avoidance Motivation.

As was the case with Self-Efficacy and Training, a noticeable number of respondents did not agree with or were neutral about top management's support in protecting the DHIS against cyber-attacks, and the related discussion regarding this given in Section 5.10 applies here as well. A suggestion is made that this reflects a considered response based on first-hand experience by the people completing the questionnaire. Section 5.7.6 and Figure 5.4 present the descriptive statistics for the set of questions regarding training.

The results of this hypothesis test were supported by both the correlation analysis (Table 5.16) and the multiple regression analysis (Table 5.20). The hypothesis focused on top management's support in protecting the organisation against cyber-attacks, positively impacting the employees' motivation to protect the organisation against cyber-attacks. Results show that top management support is significantly related to cyber-attack avoidance motivation. This includes investing in financial resources to prevent cyber-attacks as well as investing in information technology to ensure that DHIS is secured against cyber-attacks. Hasan, Ali, Kurnia and Thurasamy (2021) agree that top management support has a positive impact on safeguarding the organisation against cyber-attacks.

In contrast, these results did not agree with those of others; studies done by Jones et al. (2010) and Wang et al. (2010) which show no relationship between Top Management Support on safeguarding the organisation against cyber-attacks.

H7: Increased levels of Perceived Ease of Use has an increased positive impact on Cyber-attack Avoidance Motivation.

Tables 5.16 and 5.20 show a positive and significant relationship between the Perceived Ease of Use and *Cyber-attack Avoidance Motivation*. The hypothesis tested proved a strong relationship between Perceived Ease of Use of the DHIS (not of security software) and Cyber-attack Avoidance Motivation. The descriptive statistics (Section 5.7.7) indicate that users agree

that DHIS is easy to use and can assist them in carrying out their daily tasks. It is very likely that the responses given to this set of questions are based on first-hand experience. The findings of this hypothesis are the same as those done by Al-Zahrani (2020), Addae et al. (2019) and Sylvester (2022) since they also discovered that Perceived Usefulness is significant in achieving improved compliance with technology threat avoidance.

H8: Increased levels of Perceived Usefulness has an increased positive impact on Cyber-attack Avoidance Motivation.

The descriptive statistics (Section 5.7.8) indicate that users agree unambiguously that the DHIS is very useful and can assist them in carrying out their daily tasks. It is very likely that the responses given to this set of questions are based on first-hand experience. Hypothesis testing results from the correlation analysis only supported that Perceived Usefulness is significant in promoting Cyber-attack Avoidance Motivation. This is consistent with the study done by Al-Zahrani, 2020; Addae et al., 2019; Sylvester, 2022) since they discovered that Perceived Ease of Use is significant.

The findings from the multiple regression analysis are similar to those done by Al-Zahrani (2020) and Addae et al. (2019) since they also discovered that Perceived Usefulness is insignificant.

The findings from the multiple regression analysis conflict with those done by Al-Zahrani (2020) and (Addae et al., 2019) as they discovered that Perceived Usefulness would positively influence cyber-attack avoidance. As noted above, the correlation analysis for the study reported here agrees with these findings, but the multiple regression analysis is considered to be a more valuable result.

6.4 Summary of the conceptual research framework

The aim of this investigation set out to identify the most efficient means of promoting adherence to the District Health Information System's (DHIS) cyber-security regulations. To achieve this goal, the researcher investigated how Tshwane District Healthcare Centres workers who deal with the DHIS on a daily basis view dangers from cyberattacks. The study made use of a conceptual framework whose core constructs were adopted from (TAM, TOE, and TTAT). A conceptual framework was developed to achieve the research purpose using related hypotheses. Empirical research data were collected and quantitatively examined using SSPS version 26. Supported hypotheses (H5, H6 and H7) were therefore used to develop the final conceptual framework, as indicated in Figure 6.1.

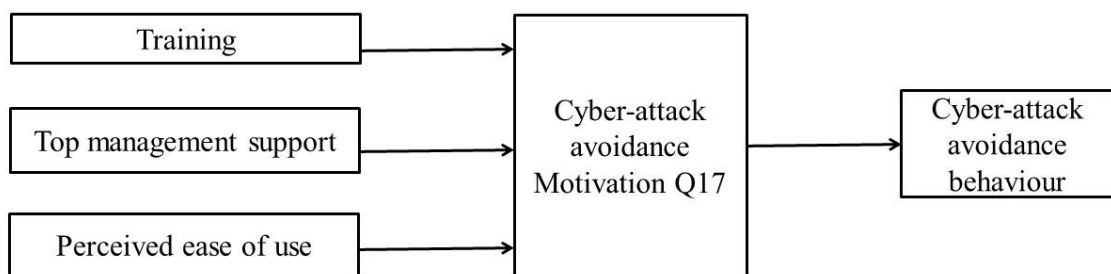


Figure 6.1: Final Conceptual Framework

6.4.1 The theoretical contribution of the study

Several cybersecurity-related problems afflict the healthcare sector. These problems range from distributed denial of service (DDoS) assaults that impair hospitals' ability to deliver patient care to malware that compromises the security of systems and the privacy of patients. The study contributed to the body of knowledge by developing a conceptual framework for information system research. This framework can be used as a guide that healthcare centres can follow to improve compliance with the measures in place to prevent cyber-attacks on their systems. The theoretical contribution of this study was derived from the literature on Information Systems theories to evaluate the factors that increase motivation to minimise the threat of cyber-attacks and, in so doing, bring about behaviour change and improve the effectiveness of cyber-security controls in DHIS. This is in line with the widely accepted Technology Acceptance Model that says that Attitude Towards Use, which in turn influences

Behavioural Intention to Use, leads to Actual Systems Use (Davis, 1989). In the case of this study, Attitude Towards Use and Behavioural Intention to Use are seen as being similar to Cyber-Attack Avoidance Motivation. Cyber-attach Avoidance Behaviour is similar to Actual Systems Use, and as is the case with TAM studies based on questionnaires, there was no attempt made to collect data regarding actual use.

The study discovered through this body of literature that Perceived Severity, Perceived Susceptibility, Perceived Effectiveness, Self-Efficacy, Training, Top Management Support, Perceived Ease of Use, and Perceived Usefulness could all have an impact on Cyber-Attack Avoidance Motivation. The research carried out, however, reduced this to Training, Top Management Support and Perceived Ease of Use, all have an impact on Cyber-Attach Avoidance Motivation in the environment of District Healthcare Centres in Tshwane.

As noted in the discussion in Section 5.1, a good theory is logical, has high explanatory power, is falsifiable and has only a small number of constructs (is simple and parsimonious). The logical structure comes from building on existing theories; the theory is coherent. The explanatory power is made evident by using multiple regression and assists researchers in explaining known findings. Falsifiability (or being testable) is a feature of positivist, quantitative research. The parsimony or simplicity resulted from retaining only of factors that do not overlap with others. The result of these characteristics should be a theory that is generalizable. The current study was an attempt to achieve these goals for a good theory, but limitations are acknowledged in Section 6.5.

6.4.2 The methodological contribution of the study

A conceptual framework that can be developed utilising a methodical approach was developed (see Figure 6.1). The actions taken to identify research participants, collecting data by means of a survey delivered to identify volunteers individually via a link, and analysis of the study's quantitative data were the study's methodological contributions. A positivist approach was followed. This methodology is not new and has been applied in other studies within the information system context.

The initial structural model included the following variables: Perceived Severity, Perceived Susceptibility, Perceived Effectiveness, Self-Efficacy, Training, Top Management Support,

Perceived Ease of Use and Perceived Usefulness which can all have an impact on the dependent variable Cyber-Attack Avoidance Motivation. In order to avoid cyber-attacks on DHIS, a revised conceptual framework (see Figure 6.1) for the efficiency of cyber-security controls was developed as part of the methodological contribution.

6.4.3 The practical contribution of the study

The study contributed to protecting the healthcare industry's sensitive data from cyber-attacks by developing a conceptual framework that may be used as a guideline to minimise the occurrence of cyber-attacks due to the 'people factor' of end users not being sufficiently conscientious about taking the prescribed protective steps against criminal intrusion into the system. This was the study's primary contribution.

The development of a conceptual framework enhanced the body of knowledge's theoretical components. Future researchers who might want to look into ways to improve the efficacy of cyber-security measures in other systems can use this conceptual framework. The study also provided guiding principles for encouraging the use of cyber-security policies and control measures to prevent cyber-attacks. The study offered a better comprehension of how to adequately safeguard the DHIS. In order to promote cyber-attack avoidance behaviours in DHIS, the study also made a significant contribution by laying out guiding principles for how acceptance of cyber-security controls by DHIS users should be encouraged, monitored, evaluated, and used effectively at the Tshwane District Healthcare Centres.

6.5 Limitations of this study

Limitations are shortcomings, influences or situations that can compromise the outcome of the research and are out of the researcher's control and have constraints on the outcome. In all research projects, certain limitations are encountered that could also contribute to how the research is undertaken. The limitations or constraints are numerous, but they are associated with undergoing any research. The existing time constraints are a feature of research done as part of a postgraduate degree programme. The time restrictions relate to the amount of time available to gather the data needed for output. Furthermore, the cost of travelling to gather and purchase data is a cost restriction. The healthcare support staff from the hospitals in the

Tshwane district were included as the study population. However, due to their hectic schedules, several of these healthcare support staff were unable to engage in this study, which reduced the overall number of study participants.

In addition, the quality of data gathered and its potential influence on findings were also found to be limitations for this study. Self-reported data collected by self-administered questionnaires tend to be optimistic and non-controversial. There was some evidence of this particularly for questions about factors that the respondents had little first-hand experience. It was also noted that some factors might possibly overlap, such as perceived ease of use and self-efficacy.

6.6 Future research

Risk analyses can often be performed to evaluate the system's vulnerability (susceptibility). User training on both the DHIS system and cyber-security will benefit users to have confidence in using the system and following effective measures to prevent cyber-attacks on the DHIS. Furthermore, it was suggested that cyber-security awareness training be provided promptly because the majority of the data collectors are individuals who have completed grade 12 and frequently utilise the DHIS system. In addition, frequent system maintenance is necessary to reduce the risk of cyber-attacks on DHIS.

6.7 Recommendations

The study has identified several recommendations from the literature, not all of which were explicitly covered in the empirical research. These broadly address research objectives 1 and 2.

The need for employee IT skills: The cyber-security sector suffers from a severe skills gap. These result in issues with IT knowledge needed to create effective cyber-security controls in DHIS to defend against cyber-attacks endangering personal privacy, national security, and the economy. The main question to this gap is what needs to be done to install IT personnel with relevant skills to fight cyber-crimes. Healthcare sectors lack IT skilled personnel in numbers (Caldwell, 2013).

The need for cyber-security awareness: Although end users are not required to install or maintain standard security software such as firewalls or antivirus software on computers at work, the user is still the weakest link regarding cyber-security and are targeted by cyber-criminals via email or Internet web sites that they interact with. Even though some initiatives on cyber-security awareness exist, users are ignorant and pose the systems to cyber-attacks. They can be easily tricked by cyber-criminals simply by just sending a phishing email, and the user will open that link leaving the system vulnerable to attacks. Teams for responding to cyber-security incidents have been established in South Africa (CSIRTs) to create nationwide awareness campaigns for other organisations. This was put into place to assist organisations in alerting people to current threats (Ahmed et al., 2017).

The need for an increase in ways of countering attacks: Different strategies and frameworks are needed to fight cyber-crimes; however, there is an increase in cyber-attacks across the globe in healthcare centres. This is a global problem.

The need for policies and strategies: There is a lack of effective cyber-security policies and frameworks within the healthcare sector in South Africa. South Africa has implemented a National cyber-security strategy to fight cyber-crimes in the public and private sectors, but it is ineffective (South African National Department of Health, 2012).

The need for effective cyber-security controls: There is a lack of effective cyber-security controls in the healthcare sector (Chen, Lambright & Abdelwahed, 2016). Healthcare is one of the industries that cyber-criminals have recently targeted, and there are little to no cyber-security measures in place to stop cyber-attacks in this sector (Zriqat & Altamimi, 2016). This is because cyber-criminals primarily targeted financial organisations in the past year, hardly attacking the healthcare sector (Health, 2012).

6.8 Conclusion

The study has shown that DHIS is vulnerable to cyber-attacks due to the interconnection of the system and the web. These vulnerabilities affect the healthcare sector since the system is critical and contains confidential medical information. Implementing effective cyber-security controls requires collaboration between end users, top management and cyber-security-skilled personnel. The entire healthcare system might be affected by a cyber-attack on the DHIS. This study discovered that because medical data is so important, fraudsters are focusing on it.

Furthermore, more solutions must be developed to combat cyber-attacks in healthcare sectors and other industries. This study's conceptual framework offers the ability to defend against cyber-attacks on DHIS. This study also revealed that healthcare institutions must spend money on cyber-security training for end users to guarantee the efficacy of DHIS security. Furthermore, constant review and audits are essential to ensure that implemented cyber-security controls are still effective and relevant, as cyber-criminals constantly find new ways to exploit the systems.

References

- Addae, J. H., Sun, X., Towey, D. and Radenkovic, M., 2019. Exploring user behavioral data for adaptive cybersecurity. *Exploring user behavioral data for adaptive cybersecurity*, 29(1), p. 33.
- Adom, D., Hussein, E. K. and Agyem, J. A., 2018. Theoretical and conceptual framework: mandatory ingredients of a quality research. *International Journal of Scientific Research*, 7(1) pp. 438-441.
- Africa Tech, 2018. *SA has the third highest number of cyber crime victims worldwide*, Durban: IOL. [Online] <https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/> [Accessed 14 02 2021].
- Ahmed, H., Alsadoon, A., Prasad, P. W. C., Costadopoulos, N., Hoe, L. S. and Elchoemi, A., 2017. Next generation cyber security solution for an ehealth organization. In *2017 5th International Conference on Information and Communication Technology (ICoICT)* (pp. 1-5). IEEE.
- Ali, N., Samsuri, S., Seman, M. A., Brohi, I. and Shah, A., 2018. Cybercrime an emerging challenge for internet users: An overview. *Sindh University Research Journal (Science Series)*, 50(3D), pp. 55-58.
- Allen, E., 2016. *Chino Valley Medical Center Attacked with Ransomware*. [Online] Available at: <https://techtalk.pcmatic.com/2016/03/25/chino-valley-medical-center-attacked-with-ransomware/> [Accessed 14 02 2021].
- Al-Zahrani, M. S., 2020. Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia. *International Journal of Electrical and Computer Engineering (IJECE)*, 10(5), pp. 10-11.
- Anderson, C. L. and Agarwal, R., 2010. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, pp. 613-643.
- Asiamah, N., Mensah, H. K. and Oteng-Abayie, E. F., 2017. General, target, and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report*, 22(6), pp.1607-1621.
- Assegaff, S., 2014. A Literature Review: Acceptance Models for e-learning Implementation in Higher Institution. 2014 International Conference on Advances in Education Technology (ICAET-14), (pp. 86-89). Atlantis Press.
- Baker, J., 2012. The Technology–Organization–Environment Framework. In: Y. K. Dwivedi, M. R. Wade and S. L. Schneberger, eds. *Information Systems Theory: Explaining and Predicting*. New York: Springer, pp. 255-260.
- Bandura, A., 1982. Self-efficacy mechanism in human agency. *American Psychologist*, 37(2), p.122.

- Bandura, A., 1988. Organisational applications of Social Cognitive Theory. *Australian Journal of management*, 13(2), pp. 275-302.
- Bartlett, J. E., Kotrlik, J. W. and Higgins, C. C., 2001. Organisational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, 19(1), pp. 43-50.
- Batchelor, B. and Wazvaremhaka, T., 2019. Balancing financial inclusion and data protection in South Africa: Black Sash Trust v Minister of Social Development. *South African Law Journal*, 136(1), pp. 112-130.
- Bhattacharjee, A., 2012. *Social science research: Principles, methods, and practices*. Digital Commons @ University of South Florida.
- Bendovschi, A., 2015. Cyber-Attacks – Trends, Patterns and security countermeasures. *Procedia Economics and Finance*, 28, pp. 24 – 31.
- Bigsby, E. and Albarracín, D., 2022. Self- and response efficacy information in fear appeals: A meta-analysis. *Journal of Communication*, 72(2):241-63.
- Buch, R., Ganda, D., Kalola, P. and Borad, N., 2017. World of cyber security and cybercrime. *Recent Trends in Programming Languages*, 4(2), pp. 18-23.
- Butt, U. J., Abbod, M., Lors, A., Jahankhani, H., Jamal, A. and Kumar, A., 2019. Ransomware threat and its impact on SCADA. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 205-212). IEEE.
- Caldwell, T., 2013. Plugging the cyber-security skills gap. *Computer Fraud and Security*, 2013(7), pp. 5-10.
- Camara, C., Peris-Lopez, P. and Tapiador, J. E., 2015. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*, 55, pp. 272-289.
- Carpenter, D., Young, D. K., Barret, P. and McLeod, A. J., 2019. Refining Technology Threat Avoidance Theory. *Communications of the Association for Information Systems*, 44(22), pp. 380-407.
- CBS-NEWS, 2017. *Inside the New York hospital hackers took down for 6 weeks*. [Online] Available at: <https://www.cbsnews.com/news/cbsn-on-assignment-hackers-targeting-medical-industry-hospitals/> [Accessed 07 02 2021].
- Chen, H. and Li, W., 2017. Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security*.
- Chen, D. Q. and Sylvester, H., 2019. Wishful thinking and IT threat avoidance: An extension to the Technology Threat Avoidance Theory. *IEEE Transactions On Engineering Management*, 66(4), pp. 552-567.

- Chen, Q., Lambright, J. and Abdelwahed, S., 2016, June. Towards autonomic security management of healthcare information systems. In 2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) (pp. 113-118). IEEE.
- Chenoweth, T., Minch, R. and Gattiker, T., 2009. Application of Protection Motivation Theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences - 2009*, pp. 1-10. IEEE.
- Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE Access*, 7, pp. 74361-74382.
- Chiew, K. L., Yong, K. S. C. and Tan, C. L., 2018. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems With Applications*, 106, pp. 1-20.
- Clubb, A. C. and Hinkle, J. C., 2015. Protection Motivation Theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, 28(3), pp. 336-355.
- Cohen, L., Manion, L., & Morrison, K. (2007). *Research Methods in Education* (6th ed.). Routledge.
- Coventry, L. and Branley, D., 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113 48–52.
- Creswell, J. and Plano Clark, V., 2011. *Designing and Conducting Mixed Methods Research*. Los Angeles. : Sage Publications.
- Creswell, J. W. and Creswell, J. D., 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. United Kingdom: SAGE Publications, Inc.
- Daniel, J., 2012. *Sampling Essentials: Practical Guidelines for Making Sampling Choices*. Los Angeles: Sage.
- Davis, F. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13, 319-340. <https://doi.org/10.2307/249008>
- Davis, J., 2016a. *Ransomware attack on dermatology office breaches more than 13,000 patient records*. [Online] Available at: [healthcareitnews.com/news/ransomware-attack-dermatology-office-breaches-more-13000-patient-records](https://www.healthcareitnews.com/news/ransomware-attack-dermatology-office-breaches-more-13000-patient-records) [Accessed 14 02 2021].
- Davis, J., 2016b. *Ransomware attack on Urgent Care Clinic of Oxford, purportedly caused by Russian hackers*. [Online] Available at: <https://www.healthcareitnews.com/news/ransomware-attack-urgent-care-clinic-oxford-purportedly-caused-russian-hackers> [Accessed 14 02 2021].

- Davis, J., 2016c. *Two providers forced to pay up in ransomware attacks*. [Online] Available at: <https://www.healthcareitnews.com/news/two-more-ransomware-attacks-both-organizations-pay> [Accessed 14 02 2021].
- Davis, J., 2021a. *Actor exploits Beaumont Health's COVID-19 vaccine scheduling tool*. [Online] Available at: <https://healthitsecurity.com/news/actor-exploits-beaumont-healths-covid-19-vaccine-scheduling-tool> [Accessed 18 February 2021].
- Davis, J., 2021b. *Hackers Leak COVID-19 Vaccine Data Stolen During EU Regulator Breach*. [Online] Available at: <https://healthitsecurity.com/news/hackers-leak-covid-19-vaccine-data-stolen-during-eu-regulator-breach> [Accessed 18 February 2021].
- Davis, J., 2021c. *Healthcare accounts for 79% of all reported breaches, attacks rise 45%*. [Online] Available at: <https://healthitsecurity.com/news/healthcare-accounts-for-79-of-all-reported-breaches-attacks-rise-45> [Accessed 18 February 2021].
- Department of Justice and Constitutional Development, 2018. Information Regulator Protection of Personal Information Act 2013 (Act No. 4 of 2013). *Government Gazzet 14 December 2018*, pp. 2-15.
- Dibaji, S. M., Pirani, M., Flamholz, D. B., Annaswamy, A. M., Johansson, K. H. and Chakraborty, A., 2019. A systems and control perspective of CPS security. *Annual Reviews in Control*, 47, pp. 394-411.
- Djenna, A. and Saïdouni, D. E., 2018. Cyber attacks classification in IoT-based-healthcare infrastructure. *2018 2nd Cyber Security in Networking Conference (CSNet)*, pp. 1-4. IEEE.
- Du Plooy-Cilliers, F., Davis, C. and Bezuidenhout, R. M., 2014. *Research Matters*. 1st ed. Claremont Cape Town: Juta limited.
- Dyrda, L., 2020. *The 5 most significant cyberattacks in healthcare for 2020*. [Online] Available at: <https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html> [Accessed 07 02 2021].
- Ehizibue, D., 2022. Investigation of individuals' behavior towards phishing attacks using the health belief model (Bachelor's thesis, University of Twente).
- Els, F. and Cilliers, L., 2018. A privacy management framework for personal electronic health records. *African Journal of Science, Technology, Innovation and Development*, 2018, 10(6), pp. 725-34.

- Fortified, 2021. *2021 Horizon Report The State of Cybersecurity in Healthcare*, USA: Horizon Report. <https://fortifiedhealthsecurity.com/horizonreports/2021-horizon-report/> Accessed [10 02 2022]
- Furusa, S. S. and Coleman, A., 2018. Factors influencing e-health implementation by medical doctors in public hospitals in Zimbabwe. *South African Journal of Information Management*, 20(1), pp. 1-9.
- Gravetter, F. J. and Wallnau, L. B., 2017. *Statistics for the Behavioral Sciences*. 10 th ed. Canada: Cengage Learning.
- Grossman, V. A., 2020. Catastrophe in radiology: Considerations beyond common emergencies. *Journal of Radiology Nursing*, 39(4), pp. 336-346.
- Hammersley, M. 2004. *Social Research Philosophy, Politics and Practice*. 7th ed. London: Sage Publications.
- Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R., 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications Applications*, 58, p. 102726.
- Heo, M., Kim, N. and Faith, M. S., 2015. Statistical power as a function of Cronbach alpha of instrument questionnaire items. *BMC Medical Research Methodology*, 15(1), pp.1-9.
- Huizingh, E. K. R. E., 2007. *Applied Statistics with SPSS*. 1st ed. London: SAGE Publications Inc.
- Ismail, W.N.S.W. and Ali, A., 2013. Conceptual model for examining the factors that influence the likelihood of Computerised Accounting Information System (CAIS) adoption among Malaysian SMEs. *International Journal of Information Technology and Business Management*, 15(1), pp.122-151.
- Iyamu, T. and Ngqame, Y., 2017. Towards a conceptual framework for protection of personal information from the perspective of Activity Theory. *South African Journal of Information Management*, 19(1), pp.1-7.
- Jang-Jaccard, J. and Nepal, S., 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), pp.973-993.
- Jideani, P., Leenen, L., Alexander, B. and Barnes, J., 2018, August. Towards an electronic retail cybersecurity framework. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (IcABCD)* (pp. 1-6). IEEE.
- Kandeh, A. T., Botha, R. A. and Fatcher, L. A., 2018. Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *South African Journal of Information Management*, 20(1), pp. 1-9.

- Khan, A., 2017. *IS Theory Technology Threat Avoidance Theory (TTAT)*. [Online] Available at: https://is.theorizeit.org/wiki/Technology_Threat_Avoidance_Theory [Accessed 05 11 2019].
- Khan, M. T., Serpanos, D. and Shrobe, H., 2018, October. Highly assured safety and security of e-health applications. In 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)(pp. 137-144). IEEE.
- Kim, Y. and Kim, B., 2021. The effective factors on continuity of corporate information security management: Based on TOE Framework. *Information*, 12(11), p.446.
- Kim, Y., Kim, I. and Park, N., 2013. Analysis of cyber attacks and security intelligence. *Mobile, Ubiquitous, and Intelligent Computing*, 274, p.489.
- Kivunja, C. and Kuyini, A. B., 2017. Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5), pp.26-41.
- Krisby, R. M., 2018. Health care held ransom: Modifications to data breach security and the future of healthcare privacy protection. *Health Matrix*, 28(1), pp. 365-400.
- Kruse, C. S., Frederick, B., Jacobson, T. and Monticone, D. K., 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), pp. 1-10.
- Labuschagne, W. A., Burke, I., Veerasamy, N. and Eloff, M. M., 2011. Design of cyber security awareness game utilizing a social media framework. In *2011 Information Security for South Africa*, pp. 1-9. IEEE.
- Leedy, P. D. and Ormrod, J. E., 2005. *Practical research* (108). Saddle River, NJ, USA: Pearson Custom.
- LaRose, R. and Rifon, N. J., 2007. Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, 41(1), pp.127-149.
- Liang, H. and Xue, Y., 2009. Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), pp. 71-90.
- Luiten, A., Hox, J. and de Leeuw, E., 2020. Survey nonresponse trends and fieldwork effort in the 21st century: Results of an international study across countries and surveys. *Journal of Official Statistics*, 36(3), pp.469-487.
- Luna, R., Rhine, E., Myhra, M., Sullivan, R. and Kruse, C.S., 2016. Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), pp.1-9.
- Mabunda, S., 2019. Cyber extortion, ransomware and the South African Cybercrimes and Cybersecurity Bill. *Statute Law Review*, 40(2), pp.143-154.

- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), pp. 469–479. [https://doi.org/10.1016/0022-1031\(83\)90023-9](https://doi.org/10.1016/0022-1031(83)90023-9)
- Mahindra, E. and Whitworth, B., 2005. The web of system performance: Extending the TAM model. *AMCIS 2005 Proceedings*, p.173.
- Mangena, D., 2016. Will legislation protect your virtual space? Discussing the draft Cybercrime and Cyber Security Bill. *De Rebus*, 2016 (560), pp.33-34.
- Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T. and Hubaux, J.P., 2013. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3), pp.1-39.
- Mapimele, F. and Bokang, C.M., 2019, February. The cybercrime combating platform. In 14th International Conference on Cyber Warfare and Security, ICCWS(pp. 237-242).
- Marjanovic, Z., 2013. Effectiveness of security controls in BYOD environments. *The University of Melbourne*. <http://hdl.handle.net/11343/33346>.
- Matthews, T., 2019. *Creeper: The World's First Computer Virus*. [Online] Available at: <https://www.exabeam.com/information-security/creeper-computer-virus/> [Accessed 14 11 2020`].
- McCarthy, J., 2016. *Hackers hit another hospital with ransomware, encrypt four computers*. [Online] Available at: <https://www.healthcareitnews.com/news/hackers-hit-another-hospital-ransomware-encrypt-four-computers> [Accessed 14 02 2021].
- McGregor, S. L. T., 2019. Research Methodologies. In: *Understanding and Evaluating Research: A Critical Guide*. Thousand Oaks: SAGE Publications, Inc, pp. 21-50.
- Menard, P., Bott, G. J. and Crossler, R. E., 2017. User motivations in protecting information security: Protection Motivation Theory versus Self-Determination Theory. *Journal of Management Information Systems*, 34(4), pp.1203-1230.
- Miliard, M., 2016. *Two more hospitals struck by ransomware, in California and Indiana*. [Online] Available at: <https://www.healthcareitnews.com/news/two-more-hospitals-struck-ransomware-california-and-indiana> [Accessed 14 02 2021].
- Minister of Justice and Correctional Services, 2016. *CyberCrimes and CyberSecurity Bill*, Pretoria: *Government Gazette No. 40487 of 9 December 2016*.
- Minister of State Security, 2015. *National CyberSecurity Policy Framework for South Africa*. *Government Gazzette 4 December 2015*, pp. 6-23.

- Mitrovic, Z., 2018. *Can BRICS boost cybersecurity of its member countries?*. [Online] Available at: <http://vmadvisory.com/cybercrime/> [Accessed 06 October 2019].
- Mohamed, N. and Ahmad, H., 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), pp.2366-2375.
- Monegain, B., 2016a. *Hackers hit two California hospitals with ransomware*. [Online] Available at: <https://www.healthcareitnews.com/news/hackers-hit-two-california-hospitals-ransomware> [Accessed 14 02 2021].
- Monegain, B., 2016b. *Methodist Hospital recovering from five day ransomware attack, claims it did not pay up*. [Online] Available at: <https://www.healthcareitnews.com/news/methodist-hospital-recovering-five-day-ransomware-attack-claims-it-did-not-pay> [Accessed 14 02 2021].
- Monegain, B., 2016c. *University of Southern California hospitals recover from ransomware attack*. [Online] Available at: <https://www.healthcareitnews.com/news/university-southern-california-hospitals-recover-ransomware-attack> [Accessed 14 02 2021].
- Morgan, G.A., Barrett, K.C., Leech, N.L. and Gloeckner, G.W., 2019. *IBM SPSS for introductory statistics: Use and interpretation: Use and interpretation*. Routledge.
- Morse, A. 2017. *Investigation: WannaCry cyber attack and the NHS*, London: National Audit Office, Department of Health.
- Mungadze, S., 2020a. *Life Healthcare Group hit by cyber attack amid COVID-19*. [Online] Available at: <https://www.itweb.co.za/content/JBwErVnBK4av6Db2> [Accessed 08 February 2021].
- Mungadze, S., 2020b. *Life Healthcare reveals damage caused by data breach*. [Online] Available at: <https://www.itweb.co.za/content/rW1xLv59YPGvRk6m> [Accessed 08 02 2021].
- Myers, M., 2013. *Qualitative Research in Business and Management*. 2nd ed. London: Sage Publications.
- Naik, S., 2021. *SA hospitals under further strain due to increase in cyber attacks*. [Online] Available at: <https://www.iol.co.za/saturday-star/news/sa-hospitals-under-further-strain-due-to-increase-in-cyber-attacks-efb62b96-9170-43e9-b1af-475783472ba9> [Accessed 08 February 2021].
- Ng, B.Y., Kankanhalli, A. and Xu, Y.C., 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), pp.815-825.

- Nissan, N., Roughgarden, T., Tardos, E. and Vazirani, V. V., 2007. Combinatorial Algorithms for market equilibria. In: N. Nissan et al, ed. *Algorithm in Game Theory*. Cambridge: Cambridge University, pp. 124-144.
- NortonLifeLock, 2020. *When Were Computer Viruses First Written, and What Were Their Original Purposes?*. [Online] Available at: <https://us.norton.com/internetsecurity-malware-when-were-computer-viruses-first-written-and-what-were-their-original-purposes.html> [Accessed 14 11 2011].
- Nunes, A., Portela, F. and Santos, M. F., 2018. Improving pervasive decision support system in critical care by using Technology Acceptance Model. *Procedia Computer Science*, 141, pp. 513-518.
- Nurqamarani, A. S., Sogiarto, E. and Nurlaeli, N., 2021. Technology adoption in small-medium enterprises based on technology acceptance model: a critical review. *Journal of Information Systems Engineering and Business Intelligence*, 7(2), pp.162-172.
- Oliveira, T. and Martins, M. F., 2011. Literature review of information technology adoption models at firm level. *The Electronic Journal Information Systems Evaluation*, 14(1), pp.110-121.
- Pallant, J., 2020. *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. Routledge.
- Paul III, D. P., Spence, N., Bhardwa, N. and Coustasse, A., 2018. Healthcare facilities: Another target for ransomware attacks. Marshall University: Marshall Digital Scholar, pp. 3-10.
- Pavlik, K., 2017. Cybercrime, hacking, and legislation. *Journal of Cybersecurity Research*, 2(1), pp.13-16.
- Peng, M. H. and Hwang, H. G., 2021. An empirical study to explore the adoption of e-learning social media platform in Taiwan: An integrated conceptual adoption framework based on Technology Acceptance Model and Technology Threat Avoidance Theory. *Sustainability*, 13(17), 9946, 13(1), p.9946.
- Pitts, V., 2017. *Cyber Crimes: History of World's Worst Cyber Attacks*. India: Vij Books India Pvt Ltd, pp. 8-15.
- Powderly, H., 2016. *Hollywood Presbyterian gives in to hackers, pays \$17,000 ransom to regain control over systems*. [Online] Available at: <https://www.healthcareitnews.com/news/hollywood-presbyterian-gives-hackers-pays-17000-ransom-regain-control-over-systems> [Accessed 14 02 2021].
- Pruzan, P., 2016. Ethics and Responsibility in Scientific Research. In: *Research Methodology The Aims, Practices and Ethics of Science*. Switzerland: Springer International Publishing, pp. 273-295.

- Qamar, A., Karim, A. and Chang, P. V., 2019. Mobile malware attacks: Review, taxonomy and future directions. *Future Generation Computer Systems*, 97, pp.887-909.
- Ragan, S., 2016. *Ransomware takes Hollywood hospital offline, \$3. 6M demanded by attackers*. [Online] Available at: <https://www.csoonline.com/article/3033160/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html> [Accessed 08 October 2019].
- Rajamäki, J. and Nevmerzhitskaya, J., 2018. Cybersecurity education and training in hospitals. *IEEE Global Engineering Education Conference (EDUCON)*, pp. 2042-2046.
- Ranjit, K., 2019. *Research Methodology: A Step-by-Step Guide for Beginners*. 5th ed. London: Sage.
- Recker, J., 2013. *Scientific Research in Information Systems Research*. New York: Springer.
- Rehman, A. A. and Alharthi, K., 2016. An introduction to research paradigms. *International Journal of Educational Investigations*, 3(8), pp. 51-59.
- Rogers, R. W., 1975. A Protection Motivation Theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), pp. 93-114.
- Roy, K. C. and Chen, Q., 2020. DeepRan: Attention-based BiLSTM and CRF for Ransomware Early Detection and Classification. *Inf Syst Front*, 23, pp.299-315
- Sabillon, R., Cavaller, V., Cano, J. & Serra-Ruiz, J. 2016. Cybercriminals, cyberattacks and cybercrime. In 2016 IEEE *International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE.
- Salim, H. and Madnick, S., 2016. Cyber safety: A systems theory approach to managing cyber security risks—Applied to TJX cyber-attack. *Work. Pap. CISL 2016*, 9.
- Saunders, M., Lewis, P. and Thornhill, A., 2019. *Research Methods for Business Students*. 8th ed. New York: Pearson Professional Limited.
- Shanapinda, S., 2019. Asymmetry in South Africa's regulation of customer data protection: Unequal treatment between Mobile Network Operators (MNOs) and Over-the-Top (OTT) Service Providers. *The African Journal of Information and Communication*, 23, pp.1-20.
- Shoham, Y., 2008. Computer science and game theory. *Communications of the ACM*, 51(8), pp.74-79.
- Silva, A.A.A., Ferraz Jr, N., Guelfi, A.E., Barboza, S.H.I. and Kofuji, S.T., 2019. Grouping detection and forecasting security controls using unrestricted cooperative bargains. *Computer Communications*, 146, pp.155-173.

- Siwicki, B., 2016. *Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money.* [Online] Available at: <https://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom> [Accessed 14 02 2021].
- Slayton, T. B., 2018. Ransomware: The virus attacking the healthcare industry. *Journal of Legal Medicine*, 38(2), pp.287–311.
- Snell, E., 2017. *Healthcare Cybersecurity Attacks Rise 320% from 2015 to 2016.* [Online] Available at: <https://healthitsecurity.com/news/healthcare-cybersecurity-attacks-rise-320-from-2015-to-2016> [Accessed 18 02 2021].
- South African National Department of Health, South Africa. 2012. *National eHealth Strategy South Africa 2012-2016.* Pretoria: South African National Department of Health.
- Stehlik-Barry, K. and Babinec, A.J., 2017. *Data analysis with IBM SPSS statistics.* Packt Publishing Ltd.
- Such, J. M., Vidler, J., Seabrook, T. & Rashid, A. 2015. Cyber security controls effectiveness: a qualitative assessment of cyber essentials. Lancaster University, Lancaster.
- Sutherland, E., 2017. Governance of cybersecurity – The case of South Africa. *The African Journal of Information and Communication (AJIC)*, 20, pp. 83-112.
- Sylvester, F. L., 2022. Mobile device users' susceptibility to phishing attacks. *International Journal of Computer Science and Information Technology (IJCSIT)*, 14(1), pp. 3-4.
- Taplin, K., 2021. South Africa's PNR regime: Privacy and data protection. *Computer Law and Security Review*, 40(1), p.105524.
- Thadani, R., 2013. *The first computer virus was designed for an Apple computer, by a 15 year old.* [Online] Available at: <https://blogs.quickheal.com/the-first-pc-virus-was-designed-for-an-apple-computer-by-a-15-year-old/> [Accessed 14 11 2020].
- Timeslive, 2020. *Hackers strike at Life Healthcare, extent of data breach yet to be assessed.* [Online] Available at: <https://www.timeslive.co.za/news/south-africa/2020-06-09-hackers-strike-at-life-healthcare-extent-of-data-breach-yet-to-be-assessed/> [Accessed 08 February 2021].
- Tredoux, C. and Durrheim, K., 2013. Numbers, hypotheses & conclusions: A course in statistics for the social sciences. 2nd ed. Juta and Company Ltd.
- Tsai, C.Y., Shih, W.L., Hsieh, F.P., Chen, Y.A., Lin, C.L. and Wu, H.J., 2022. Using the ARCS model to improve undergraduates' perceived information security protection motivation and behavior. *Computers & Education*, 181, p.104449.

- Van Bavel, R., Rodríguez-Priego, N. and José Vila, P. B., 2019. Using Protection Motivation Theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, 123, pp. 29-39.
- Van Dijk, M., Juels, A., Oprea, A. and Rivest, R. L., 2013. FlipIt: The game of “stealthy takeover”. *Journal of Cryptology*, 26, pp. 655-713.
- Van Niekerk, B., 2017. An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20, pp.113-132.
- Vance, A., Siponen, M. and Pahlila, S., 2012. Motivating IS security compliance: Insights from habit and Protection Motivation Theory. *Information & Management*, 49(3-4), pp.190-198.
- Wahyuni, D., 2012. The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, 10(1), pp.69-80.
- Wallace, S., Green, K., Johnson, C., Cooper, J. and Gilstrap, C., 2021. An Extended TOE Framework for Cybersecurity Adoption Decisions. *Communications of the Association for Information Systems*, 47(2020), p.51.
- Wanyonyi, E., Rodrigues, A., Abeka, S. and Ogara, S., 2017. Effectiveness of security controls on electronic health records. *International Journal of Scientific and Technology Research*, 6(12), pp. 1-8.
- Webb, W. and Auriacombe, C., 2006. Research design in public administration : Critical considerations. *Journal of Public Administration*, 41(3), pp.588-602.
- Williams, P., 2016. *MedStar Hospitals Recovering After 'Ransomware' Hack*. [Online] Available at: <https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121> [Accessed 14 02 2021].
- Winton, R., 2016. *2 more Southland hospitals attacked by hackers using ransomware*. [Online] Available at: <https://www.latimes.com/local/lanow/la-me-ln-two-more-so-cal-hospitals-ransomware-20160322-story.html> [Accessed 14 02 2021].
- Wirth, A., 2018. The times they are a-changin': Part One. *Biomedical Instrumentation and Technology*, 52(2), pp. 148-152.
- Woon, I., Tan, G.W. and Low, R., 2005. A Protection Motivation Theory approach to home wireless security, ICIS 2005 Proceedings. 31. <https://aisel.aisnet.org/icis2005/31>
- Workman, M., Bommer, W.H. and Straub, D., 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), pp.2799-2816.

- Wu, D., 2020. Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior*, 105, p. 106229.
- Yin, R. K., 2003. *Case Study Research Design and Methods*. 5th ed. London: Sage Publications.
- You, Y., Lee, J., Oh, J. and Lee, K., 2018, January. A review of cyber security controls from an ICS perspective. In 2018 International Conference on Platform Technology and Service (PlatCon) (pp. 1-6). IEEE.
- Youn, S., 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), pp.389-418.
- Young, D., Carpenter, D. and McLeod, A., 2016. Malware avoidance motivations and behaviors: A Technology Threat Avoidance replication. *Transactions on Replication Research*, 2(1), p. 8.
- Zainal, Z., 2007. Case study as a research method. *Jurnal Kemanusiaan*, 5(1), pp. 2-4.
- Zhao, G., Cavusgil, E. and Zhao, Y., 2016. A protection motivation explanation of base-of-pyramid consumers' environmental sustainability. *Journal of Environmental Psychology*, 45, pp. 116-126.
- Zhang, L. and McDowell, W.C., 2009. Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3-4), pp.180-197.
- Zriqat, I. A. and Altamimi, A. M., 2016. Security and privacy issues in ehealthcare systems towards trusted services. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 7(9), pp.229-236.

APPENDICES

Appendix A: Gauteng Province Health Ethical Clearance Approval



Annexure 1

DECLARATION OF INTENT FROM THE PHC MANAGER FOR TSHWANE PROVINCIAL CLINICS

I give preliminary permission to **Ms Thetshelesani Netshishivhe** to do his or her research on **“The effectiveness of cybersecurity controls in District health Information Systems (DHIS) to prevent cyber-attacks: A case of Tshwane district healthcare centres”** in

ADELAIDE TAMBO CLINIC
BOEKENHOUT CHC
BOIKHUTSONG CLINIC
BOPHELONG (REGION C) CLINIC
DILOPYE CLINIC
EERSTERUST CHC
GARANKUWA VIEW CLINIC
HOLANI CLINIC
JACK HINDON CLINIC
JUBILEE GATEWAY CLINIC
KEKANASTAD CHC
KGABO CHC

KT MOTUBATSE CLINIC
LAUDIUM CHC
LOTUS GARDENS CLINIC
MANDISA SHICEKA CLINIC
MARIA RANTHO CLINIC
MERCY NGO CLINIC
NEW EERSTERUS CLINIC
PHEDISONG 1 CHC
PHEDISONG 4 CHC
PHEDISONG 6 CLINIC
RAMOTSE CLINIC
REFENTSE CHC (ODI)

SEDILEGA CLINIC
SKINNER STREET CLINIC
SOSHANGUVE 2 CLINIC
SOSHANGUVE BLOCK JJ CLINIC
SOSHANGUVE BLOCK TT CLINIC
SOSHANGUVE BLOCK X CLINIC
SOSHANGUVE CHC
STANZA BOPAPE CHC
SUURMAN CLINIC
TEMBA CHC
TLAMELONG CLINIC
WINTERVELDT CLINIC

I know that the final approval will be from the Tshwane Regional Research Ethics Committee and that this is only to indicate that the clinic/hospital is willing to assist.

Other comments or conditions prescribed by the PHC Manager to the Researcher are

The researcher to have an entry meeting with potential facilities before starting with the data collection.

Mr M. Makhudu
Primary Health Care: Tshwane

Date: 17/6/2021

Appendix B: Tshwane research committee Ethical Clearance Approval



GAUTENG PROVINCE
HEALTH
REPUBLIC OF SOUTH AFRICA

Enquiries: Dr. Manei Letebele-Hartell
Tel: +27 12 451 9036
E-mail: Troy.Mashabela@gauteng.gov.za

TSHWANE RESEARCH COMMITTEE: CLEARANCE CERTIFICATE

DATE ISSUED: 17/06/2021
PROJECT NUMBER: 43/2021
NHRD REFERENCE NUMBER: GP_202106_020

TOPIC: The effectiveness of cybersecurity controls in District health Information Systems (DHIS) to prevent cyber-attacks: A case of Tshwane district healthcare centres.

Name of the Lead Researcher: Ms Thetshelesani Netshishivhe

Name of the Supervisors: Dr. Chimbo Bester
Dr. Motsi Lovemore

Facilities: Tshwane District Facilities
(*annexure 1 attached*)

Name of the Department: UNISA

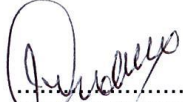
NB: THIS OFFICE REQUEST A FULL REPORT ON THE OUTCOME OF THE RESEARCH DONE AND

NOTE THAT RESUBMISSION OF THE PROTOCOL BY RESEARCHER(S) IS REQUIRED IF THERE IS DEPARTURE FROM THE PROTOCOL PROCEDURES AS APPROVED BY THE COMMITTEE.

DECISION OF THE COMMITTEE: APPROVED


.....
Dr. Mpho Moshime-Shabangu
Deputy Chairperson: Tshwane Research Committee

Date: 17/06/2021


.....
Prof. JV Ndimande
Acting Chief Director: Tshwane District Health

Date: 2021/06/17

Appendix C: UNISA Ethical Clearance Approval



UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) ETHICS REVIEW COMMITTEE

2021/05/14

Dear Ms Thetshesani Angel Netshishivhe

ERC Reference #: 2021/CSET/SOC/016

Name: Thetshesani Angel Netshishivhe

Student #: 54901995

Staff #:

**Decision: Ethics Approval from
2021/05/14 for three years
Humans involved.**

Researcher(s): Ms Thetshesani Angel Netshishivhe
54901995@mylife.unisa.ac.za, 083 423 1292

Supervisor (s): Prof Bester Chimbo
chimbb@unisa.ac.za, 011 670 9105

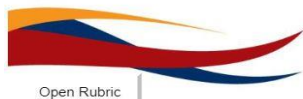
Working title of research:

**The effectiveness of cybersecurity control in District health Information Systems
(DHIS) to prevent
cyber-attacks: A case of Tshwane district healthcare centres**

Qualification: MSc in Information Systems

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Ethics Review Committee for the above mentioned research. Ethics approval is granted for 3 years.

*The **low risk application** was expedited by the College of Science, Engineering and Technology's (CSET) Ethics Review Committee on 2021/05/14 in compliance with the Unisa Policy on Research Ethics and the Standard Operating Procedure on Research Ethics Risk Assessment. The decision will be tabled at the next Committee meeting for ratification.*



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

The proposed research may now commence with the provisions that:

1. The researcher will ensure that the research project adheres to the relevant guidelines set out in the Unisa COVID-19 position statement on research ethics attached.
2. The researcher(s) will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
3. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study should be communicated in writing to the College of Science, Engineering and Technology's (CSET) Ethics Review Committee.
4. The researcher(s) will conduct the study according to the methods and procedures set out in the approved application.
5. Any changes that can affect the study-related risks for the research participants, particularly in terms of assurances made with regards to the protection of participants' privacy and the confidentiality of the data, should be reported to the Committee in writing, accompanied by a progress report.
6. The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study. Adherence to the following South African legislation is important, if applicable: Protection of Personal Information Act, no 4 of 2013; Children's act no 38 of 2005 and the National Health Act, no 61 of 2003.
7. Only de-identified research data may be used for secondary research purposes in future on condition that the research objectives are similar to those of the original research. Secondary use of identifiable human research data require additional ethics clearance.
8. No field work activities may continue after the expiry date *expiry date*. Submission of a completed research ethics progress report will constitute an application for renewal of Ethics Research Committee approval.
9. *Permission to conduct research involving UNISA employees, students and data should be obtained from the Research Permissions Subcommittee (RPSC) prior to commencing field work.*
10. *Permission to conduct this research should be obtained from the [company, CE organisation, DoE, etc name] prior to commencing field work.*

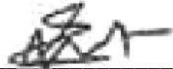
Note

The reference number 2021/CSET/SOC/016 should be clearly indicated on all forms of communication with the intended research participants, as well as with the Committee.

Yours sincerely,



Dr D Bisschoff
Chair of School of Computing Ethics Review Subcommittee
College of Science, Engineering and Technology (CSET)
E-mail: dbischof@unisa.ac.za
Tel: (011) 471-2109



Prof. E Mnkandla
Director: School of Computing
College of Science Engineering and
Technology (CSET)
E-mail: mnkane@unisa.ac.za
Tel: (011) 670 9104



Prof. B Mamba
Executive Dean
College of Science Engineering and
Technology (CSET)
E-mail: mambabb@unisa.ac.za
Tel: (011) 670 9230



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za



Adobe Acrobat
Document

Appendix D: Participant information sheet



PARTICIPANT INFORMATION SHEET

Date : 2021-06-24

Research Title: Cyber-attack avoidance behaviour in District Health Information System (DHIS): A case of Tshwane district healthcare centres

Dear Prospective Participant

My name is Thetshesani Angel Netshishivhe, and I am researching the cybersecurity of DHIS with Dr. Bester Chimbo and Dr. Lovemore Motsi, Senior lecturers in the Department of Computing towards a Master's degree at the University of South Africa (UNISA). We are kindly inviting you to participate in a study entitled the effectiveness of cybersecurity controls in District Health Information system (DHIS) to prevent cyber-attacks: A case of Tshwane district healthcare centers

WHAT IS THE PURPOSE OF THE STUDY?

The purpose of this study is to evaluate the effectiveness of implemented cybersecurity controls in the District Health Information system (DHIS) with the aim of preventing cyber-attacks. These will help determine the cyber-attacks within the healthcare sector and the damage and impact these attacks can cause on patient's data. Furthermore, the study will determine how to prevent or mitigate and where possible eradicate the cyber-attacks and breaches on the District Health Information System (DHIS). This will be achieved by evaluating the common cyber-attacks in the healthcare centers and the impact or damages that could be caused by these attacks. The study will also evaluate the resilience of the current cybersecurity controls implemented on the DHIS and if these controls are effective to prevent any cyber breach. The main aim behind this study is to protect patients' sensitive data against cybercriminals by implementing effective cyber controls. The findings of the study may be used as a guide by Healthcare management to implement effective controls that will combat cyber-attacks on e-health systems, particularly the DHIS system across South Africa.



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

WHY AM I BEING INVITED TO PARTICIPATE?

You are being invited to participate in this study because you interact with the DHIS system when working. As a result, you might be exposed to cyber threats and cyber breaches. This study is seeking about 200 participants from different healthcare centers in the Tshwane district. These participants include anyone who has access to the DHIS system.

WHAT IS THE NATURE OF MY PARTICIPATION IN THIS STUDY?

The study involves completing questionnaires. The researcher will distribute questionnaires to participants who gave consent to be part of the study. These participants will be asked questions about their experience with the District health information system and its security. The questionnaire will be Likert scale questions where participants will choose a rating from 1 to 5 ratio. The expected duration to complete the questionnaire is approximately 30 min.

CAN I WITHDRAW FROM THIS STUDY EVEN AFTER HAVING AGREED TO PARTICIPATE?

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw from this study before you hand in your questionnaire to the researcher and without giving a reason. The data collection tool is an anonymous questionnaire. This questionnaire is non-identifiable since the researcher will not ask for any personal details when completing it. Therefore, once submitted the researcher will not be able to identify who the questionnaire belongs to or submitted which questionnaire. However, you cannot withdraw participation after the submission of the online questionnaire since the researcher will not be able to identify which questionnaire belongs to which participant.

WHAT ARE THE POTENTIAL BENEFITS OF TAKING PART IN THIS STUDY?

There are no direct possible benefits for participants. The data provided by participants will assist the researcher in fulfilling the aim set out in his research study and also provide some insights into the effectiveness of cybersecurity controls to prevent cyber-attacks in the healthcare sector.

ARE THERE ANY NEGATIVE CONSEQUENCES FOR ME IF I PARTICIPATE IN THE RESEARCH PROJECT?

There are no foreseeable negative risks associated with participation in this research study. The foreseeable inconvenience for participating is your time and data. The researcher requests that you set aside time to complete the questionnaire which will be distributed to participants. The questionnaire will be distributed online as a link for participants to access it. However, this can be



done at a time convenient for you with no pressure. Therefore, there are no foreseeable risks of harm or side-effects for participating in this research.

WILL THE INFORMATION THAT I CONVEY TO THE RESEARCHER AND MY IDENTITY BE KEPT CONFIDENTIAL?

You have the right to insist that your name will not be recorded anywhere and that no one, apart from the researcher and identified members of the research team, will know about your involvement in this research. This means that your name will not be recorded anywhere, and no one will be able to connect you to the answers you provide on the questionnaire. Your answers will be given a code number, or a pseudonym and you will be referred to in this way in the data, any publications, or other research reporting methods such as conference proceedings.

Your anonymous data may be used for other purposes, such as a research report, journal articles, and/or conference proceedings. In whatever form your supplied data may be used your name and identity will always be kept confidential and private.

HOW WILL THE RESEARCHER(S) PROTECT THE SECURITY OF DATA?

Hard copies of your answers will be stored by the supervisor for a minimum period of five years in a locked cupboard/filing cabinet in Dr. Bster Chimbo's office at the University of South Africa, College of Science, Engineering, and Technology in the School of Computing located in Florida Science Campus. The storage of data for 5 years is for future research or academic purposes only. Electronic information will be stored on a password-protected computer. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. Hard copies will be shredded, and electronic copies will be permanently deleted from the hard drive of the computer through the use of a relevant software programme.

WILL I RECEIVE PAYMENT OR ANY INCENTIVES FOR PARTICIPATING IN THIS STUDY?

There are no payments or incentives for participating in this research study, participation is voluntary. Furthermore, there are no foreseeable costs that will be incurred by participating in this research study.

HAS THE STUDY RECEIVED ETHICS APPROVAL?

This study has received written approval from the Research Ethics Review Committee of the School of Computing, Unisa, and permission from the Tshwane district research. A copy of the approval letter can be obtained from the researcher if you so wish.

HOW WILL I BE INFORMED OF THE FINDINGS/RESULTS OF THE RESEARCH?



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

If you would like to be informed of the final research findings, please contact Thetshelesani Angel Netshishivhe on 083 423 1292 or email 54901995@mylife.unisa.ac.za. The findings are accessible for 5 years. Should you require any further information or want to contact the researcher about any aspect of this study, please contact 083 423 1292 email 54901995@mylife.unisa.ac.za.

Should you have concerns about how the research has been conducted, you may contact Dr. Bester Chimbo, on 011 670 9105 email chimbb@unisa.ac.za or Dr. Lovemore Motsi on 011 670 9426 or email motsil@unisa.ac.za or Contact the research ethics chairperson of the School of Computing committee, socethics@unisa.ac.za if you have any ethical concerns.

Thank you for taking the time to read this information sheet and for participating in this study.
Thank you.



Thetshelesani



University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix E: Questionnaire

SoC online anonymous questionnaire template

ONLINE QUESTIONNAIRE: STAFF OF TSHWANE DISTRICT HEALTHCARE CENTRES

RESEARCH PROJECT: *Cyber-attack avoidance behaviour in District Health Information System (DHIS): A case of Tshwane district healthcare centres*

Instructions:

*Please answer all the questions as honestly as possible. The information collected for this study will be collated and analysed in order to form an accurate picture of this research project **Cyber-attack avoidance behaviour in District Health Information System (DHIS): A case of Tshwane district healthcare centres**. It will assist the researcher to make findings and propose recommendations to improve the use of information systems to prevent cyber-attacks. You do not need to identify yourself and, similarly, the researcher will uphold anonymity in that there will be no possibility of any respondent being identified or linked in any way to the research findings in the final research report. Where required please indicate your answer with a cross (X) in the appropriate box.*

Please decide whether or not to participate by choosing the appropriate option below.

Do you agree to participate in this study?	Yes	No
--	-----	----

SECTION A: DEMOGRAPHIC INFORMATION

Indicate your choice by marking the appropriate blank block with an "X".

The following questions are **for statistical purposes only**.

Q1. Gender:

Male	1	
Female	2	

Q2. Age:

20 years and below	1	
21–25 years	2	
26–30 years	3	
31–35 years	4	
36–40 years	5	
41–45 years	6	
46–50 years	7	
51 years and above	8	

Q3. What is your highest education level?

Standard 8/Grade 10 and below	1	
Standard 9/Grade 11	2	
Standard 10/Grade 12	3	
Certificate	4	
Diploma	5	
Bachelors' Degree	6	
MBCHB degree	7	
Master's degree	8	
Doctorate degree (PHD)	9	

Q4. What is your position at work?

Data capturers	1	
Information clerk	2	
IT Administrator	3	
Head of department	4	
Facility Information Officer	5	
Facility Information Manager	6	
District Information Manager	7	
Other (specify.....)	8	

SECTION B: INFORMATION SYSTEMS KNOWLEDGE

Indicate your choice by marking the appropriate blank block with an "X".

Q5. Where do you mostly access the internet from?

Home	1	
Work	2	
Internet Cafe	3	
Other (specify).....	4	

Q6. How often do you change the password on your computer?

Never	1	
Rarely	2	
Sometimes	3	
Often	4	
Always	5	

Q7. Indicate your answer to the following statements regarding the District Health Information system (DHIS).

Item	Statement	Yes	No	Don't Know
a)	Do you have access to the District Health Information System (DHIS)?	1	2	3
b)	Is the firewall on your computer enabled?	1	2	3
c)	Are you aware of your organisation's information security policy?	1	2	3
d)	Is anti-virus software currently installed on your computer?	1	2	3
e)	Is anti-virus software currently updated on your computer?	1	2	3
f)	Is anti-virus software currently enabled on your computer?	1	2	3
g)	Are you aware of cyber-attacks?	1	2	3

SECTION C: CYBER SECURITY: PART 1

Technology Threat Avoidance Theory: **Threat Appraisal and Coping Appraisal**

Q8. Indicate your level of agreement regarding the following statements on Perceived Severity.

Item	Perceived Severity	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	I believe having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me.	1	2	3	4	5
b)	If I violate DHIS's security policy, the sanctions would put me in serious trouble.	1	2	3	4	5
c)	At work, having my confidential information accessed by someone without my consent or knowledge is a serious problem for me.	1	2	3	4	5
d)	Loss of data resulting from hacking is a serious problem for me.	1	2	3	4	5
e)	Losing DHIS data as a result of opening a suspicious email attachment is a serious problem for me.	1	2	3	4	5
f)	If my computer is infected by a virus as a result of opening a suspicious email attachment, my daily work could be negatively affected.	1	2	3	4	5
g)	An information security breach in DHIS would be a serious problem for me.	1	2	3	4	5

Q9. Indicate your level of agreement regarding the following statements on Perceived Susceptibility.

Item	Perceived Susceptibility	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	I feel that my chance of receiving an email attachment with a virus is high.	1	2	3	4	5
b)	I feel that DHIS could become vulnerable to security breaches if I do not adhere to its information security policy.	1	2	3	4	5
c)	I feel that I could fall victim to a malicious attack if I fail to comply with DHIS's information security policy.	1	2	3	4	5
d)	I believe that my effort to protect DHIS's information will reduce illegal access to it.	1	2	3	4	5
e)	DHIS's data and resources may be compromised if I do not pay adequate attention to information security policies and guidelines.	1	2	3	4	5
f)	It is likely that an information security breach is occurring at DHIS.	1	2	3	4	5
g)	It is likely that DHIS's information and data is vulnerable to security breaches.	1	2	3	4	5

Q10. Indicate your level of agreement regarding the following statements on Perceived Effectiveness.						
Item	Perceived Effectiveness (Controls)	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	Complying with the information security policies in my organization will keep information system security breaches down.	1	2	3	4	5
b)	If I comply with information security policies, the chance of information security breaches occurring in organization will be reduced.	1	2	3	4	5
c)	Careful compliance with information security policies helps to avoid security problems.	1	2	3	4	5
d)	Using information security technologies is an effective way to protect confidential information.	1	2	3	4	5
e)	I can protect my information privacy better if I use privacy protection measures on DHIS.	1	2	3	4	5
f)	Utilizing privacy protection measures in DHIS works to ensure my information privacy.	1	2	3	4	5
g)	If I utilize privacy protection measures in DHIS, I am less likely to lose my information privacy.	1	2	3	4	5

Q11. Indicate your level of agreement regarding the following statements on Self-Efficacy.						
Item	Self-Efficacy	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	My organization constantly reminds me to practice its computer and Internet security policies.	1	2	3	4	5
b)	I feel confident in setting the Web browser to different security levels.	1	2	3	4	5
c)	I feel confident in handling virus-infected files.	1	2	3	4	5
d)	I feel confident in getting rid of spyware and malware from my computer.	1	2	3	4	5
e)	I feel confident in understanding terms/words relating to cyber security.	1	2	3	4	5
f)	I feel confident using different programs to protect DHIS	1	2	3	4	5
g)	I feel confident learning advanced skills to protect DHIS	1	2	3	4	5
h)	I feel confident using the user's guide when help is needed to protect DHIS.	1	2	3	4	5
i)	I have the skills to implement security measures to stop people from getting my confidential information.	1	2	3	4	5
j)	I can recognize a suspicious email attachment even if there was no one around to help me.	1	2	3	4	5

SECTION D: Technology, Organisation, Environment (TOE) Constructs

Technology, Organisation, Environment (TOE) Constructs						
Q12. Indicate your level of agreement regarding the following statements on Training.						
Item	Training	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	My organization provides extensive training to help employees improve their awareness of cyber security issues.	1	2	3	4	5
b)	Cyber security training helps users to be aware of the impact of cyber-attacks on the DHIS.	1	2	3	4	5
c)	My organization is dedicated to making sure employees are very familiar with prevention of cyber-attacks.	1	2	3	4	5
d)	My organization has a team of experts in information systems involved in preparing the content for training programs.	1	2	3	4	5
e)	Feedback from trainees is captured before, during, and after training.	1	2	3	4	5
f)	Top management and Board have attended seminars and conferences on prevention of cyber-attacks.	1	2	3	4	5
g)	I do not have the right skills to be able to protect the DHIS from cyberattacks.	1	2	3	4	5
h)	Training will help users on cyber-attack avoidance.	1	2	3	4	5
i)	User training on cyber-attack avoidance will help users to know how to respond to cyber threats.	1	2	3	4	5

Q13. Indicate your level of agreement regarding the following statements on Top Management Support.						
Item	Top Management Support	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	Top management is likely to invest on effective controls that will help prevent cyber-attack.	1	2	3	4	5
b)	Top management is willing to take risks involved in the prevention of cyber-attacks.	1	2	3	4	5
c)	Top management is likely to be interested in prevention of cyber-attacks in order to gain competitive advantage	1	2	3	4	5
d)	Top management is likely to consider the prevention of cyber-attacks as strategically important.	1	2	3	4	5
e)	Top management has allocated adequate financial and other resources for the prevention of cyber-attacks.	1	2	3	4	5
f)	Top management is highly interested in actively championing information security goals.	1	2	3	4	5

g)	Top management is aware that they have the responsibility to ensure that DHIS is protected from cyber-attacks.	1	2	3	4	5
h)	Top management believe that information technology security investments and expenditures are worthwhile.	1	2	3	4	5

Technology Acceptance Model

Q14. Indicate your level of agreement regarding the following statements on Perceived Ease of Use.

Item	Perceived Ease of Use	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	Learning to operate the DHIS would be easy for me.	1	2	3	4	5
b)	I would easily protect the information on my computer using the DHIS.	1	2	3	4	5
c)	I find the DHIS to be flexible to interact with.	1	2	3	4	5
d)	I find the DHIS to be easy to use (user friendly).	1	2	3	4	5
e)	Interacting with the DHIS does not require a lot of my mental effort.	1	2	3	4	5
f)	I find it easy to get the DHIS to do what I want it to do.	1	2	3	4	5
g)	I believe it is clear and understandable on how to use DHIS.	1	2	3	4	5
h)	I believe it is easy to get the patient information on DHIS.	1	2	3	4	5

Q15. Indicate your level of agreement regarding the following statements on Perceived Usefulness.

Item	Perceived Usefulness	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	Using the DHIS would increase the efficiency of my daily work.	1	2	3	4	5
b)	The DHIS would make it easier to keep track of any updates on security measures on my computer.	1	2	3	4	5
c)	The DHIS would allow me to better prevent any cyberattacks on my computer.	1	2	3	4	5
d)	The DHIS would be useful to me as an employee.	1	2	3	4	5
e)	Using the DHIS in my job increases my productivity.	1	2	3	4	5
f)	Using the DHIS enhances my effectiveness in my job.	1	2	3	4	5
g)	In my organization, using the DHIS will help me get patient information quickly.	1	2	3	4	5
h)	In my organization using the DHIS will keep patient data safe and secure.	1	2	3	4	5
i)	In my organization, I believe using DHIS will help doctors to make informed decisions about the patient's health.	1	2	3	4	5
j)	In my organization I believe using DHIS will have impact on healthcare service delivery.	1	2	3	4	5

Q16. Indicate your level of agreement regarding the following statements on Perceived Effectiveness.						
Item	Perceived Effectiveness (security software)	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	Security software would be useful for detecting and avoiding cyber threats on DHIS.	1	2	3	4	5
b)	Security software would increase my performance in protecting my computer from cyber threats on DHIS.	1	2	3	4	5
c)	Security software would enable me to search and avoid cyber threats on DHIS on my computer faster.	1	2	3	4	5
d)	Security software would enhance my effectiveness in searching and avoid cyber threats on DHIS on my computer.	1	2	3	4	5
e)	Security software would make it easier to search and avoid cyber threats on DHIS on my computer.	1	2	3	4	5
f)	Security software would increase my productivity in searching and avoiding cyber threats on DHIS.	1	2	3	4	5

SECTION E: Technology Threat Avoidance Theory (TTAT) Constructs: PART 2

Technology Threat Avoidance Theory: Problem-focused coping						
Q17. Indicate your level of agreement regarding the following statements on Cyber-Attack Avoidance Motivation.						
Item	Cyber-Attack Avoidance Motivation	Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
a)	I intend to use security software to avoid cyberattacks on DHIS.	1	2	3	4	5
b)	I predict I would use security software to avoid cyberattacks on DHIS.	1	2	3	4	5
c)	I plan to use security software to avoid cyberattacks on DHIS.	1	2	3	4	5
d)	I run security software updates regularly to avoid cyberattacks on DHIS.	1	2	3	4	5
e)	I have the resources and the knowledge to take the necessary security measures.	1	2	3	4	5
f)	Taking the necessary security measures is entirely under my control.	1	2	3	4	5
g)	I believe enabling security measures on DHIS will avoid security breaches.	1	2	3	4	5

Appendix F: Editor's certificate



Certificate of Editing

This is to certify that the dissertation

Cyber-attack avoidance behaviour in District Health
Information Systems (DHIS):
A case of Tshwane district healthcare centres

By

THETSHELESANI ANGEL NETSHISHIVHE

Has been proofread and has been edited for usage of English language

By

Dr Patricia M Alexander

A handwritten signature in cursive script, appearing to read 'Patricia M Alexander'.

1 Cadoza Str
Westdene
Johannesburg
Alexanderpatricia92@gmail.com
0827315322

7 March 2023

Appendix G: Turnitin Report

Turnitin Similarity score

Full Dissertation_ Final submission

ORIGINALITY REPORT

14%

SIMILARITY INDEX

11%

INTERNET SOURCES

5%

PUBLICATIONS

5%

STUDENT PAPERS

PRIMARY SOURCES
