



Title: The Enforcement of End-user Security Compliance using Chatbot

by

Goodman Mzwabantu Siyongwana

Student number: 208225609

**Thesis submitted in fulfilment of the requirements for the degree of Master of
Technology: Discipline: Information Technology in the Faculty of Informatics and Design
at the Cape Peninsula University of Technology**

Supervisor: Doctor Boniface Kabaso

Co-Supervisor: Denise Lakay

Cape Town

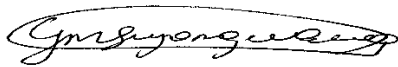
December 2022

CPUT copyright information

The thesis may not be published either in part (in scholarly, scientific or technical journals) or as a whole (as a monograph) unless permission has been obtained from the University.

DECLARATION

I, Goodman Mzwabantu Siyongwana, declare that the contents of this dissertation/thesis represent my own unaided work and that the dissertation/thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.



2022

Signed

Date

ABSTRACT

Information security is a multifaceted approach that combines technical and non-technical controls to ensure that organisations are protected against cyber-attacks. Technical security controls apply technological solutions such as firewalls, encryption, antivirus, antimalware, intrusion detection system and intrusion prevention systems. Non-technical security controls deal with security policies, procedures, and standards. Users need to be educated about these non-technical security controls for compliance and adherence.

Extant literature has noted poor security conduct and low compliance levels among users. This behaviour leads to what is known in the security realm as an insider threat. Cyber-attacks constantly evolve to keep up with the latest technology. However, low-tech attacks are still popular because manipulating the insider threat's vulnerability (human factor) does not require sophisticated techniques. Training and awareness are key to the success of information security policy. However, it has become apparent that ongoing user compliance is not easy to achieve because users have difficulties applying the contents of information security policy consistently. This difficulty, accompanied by a lack of regular security training, is seen as the primary cause of users' inconsistent security behaviour.

The research hypothesis of this study is that users who receive a constant reminder about the contents of the information security policy have a higher information security compliance behaviour than users without any form of reminder. This quantitative research study used a chatbot to test the hypothesis. The data was collected from two government entities in Cape Town. A random sampling technique was used to acquire a sample of forty-two participants. Experiments followed a two-group experimental design approach: the experimental group and the control group. The experimental group was exposed to the treatment; in this research, a chatbot was used as an intervention.

Three hypotheses were tested in this research study. The results of the first hypothesis showed a significant difference in the behaviour of the users who received training and exposure to a chatbot. The results of the second hypothesis were not statistically significant. The results of the third hypothesis proved that the compliance behaviour of users could be improved if users were to receive constant reminders about the contents of the information security policy. Implications, future research and recommendations included recommendations for a longitudinal study and extending the research to other provinces. In addition, the study recommended further analysis of information security training delivery methods.

Key Terms: Chatbot, Compliance, Information Security, Information Security Policy.

ACKNOWLEDGEMENTS

I wish to thank Jesus Christ, my Saviour, for courage and strength. My Supervisor, Professor Boniface Kabaso and Co-Supervisor, Ms Denise Lakay, for mentoring, coaching and guidance. May the Lord bless you. Professor Paul Iwuanyanwu for his invaluable input. Stephen Maduveko for support and relentless encouragement. Abed Matini. Yanga Mgoqi, Noyolo Mgwetyana and Pinky Motshware, you were all there for me when the going got tougher and always offered help and support. To Professor Ademola Abidoye, thank you for always taking the time to impart your knowledge and expertise. Finally, the Department of Human Settlements in Cape Town for showing interest in my study and agreeing to participate in the experiment.

DEDICATION

I would like to dedicate this small feat to my dearly departed father and sister. To my mother, my siblings, and Entle and Ayabukwa, the gauntlet has been thrown down by future matriarchs.

GLOSSARY

AIML	Artificial Intelligence Markup Language
AUP	Acceptable Use Policies
BYOD	Bring Your Own Device
CIA	Confidentiality Integrity and Availability
CSP	Cyber-security policies
DES	Data Encryption Standard
DL	Deep Learning
CSSB	Counterproductive Computer Security Behaviour
HCI	Human Computer Interactions
IDV	Individualism Versus Collectivism
IS	Information System
ISA	Information Security Awareness
ISP	Information Security Policy
IT	Information Technology
LSA	Latent Semantic Analysis
ML	Machine Learning
MS	Microsoft
NLP	Natural Learning Process
PARADISE	Paradigm for Dialogue System Evaluation
XML	Extensible Markup Language

PIN	Personal Identification Number
SeBIS	Security Behaviour Intentions Scale
TPB	Theory of Planned Behaviour
UAI	Uncertainty Avoidance
URL	Uniform Resource Locator

TABLE OF CONTENTS

Contents

DECLARATION.....	II
ABSTRACT.....	III
ACKNOWLEDGEMENTS.....	IV
DEDICATION.....	V
GLOSSARY.....	VI
TABLE OF CONTENTS.....	VIII
CHAPTER ONE: INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Background to the study.....	2
1.3 The Role of Chatbots in End User Security Compliance.....	3
1.4 Problem Statement.....	4
1.5 Research Aim.....	5
1.6 Objectives.....	5
1.7 Hypothesis.....	5
1.7.1 Educated Guess	5
1.7.2 Null Hypotheses H_0	6
1.7.3 Alternative Hypotheses.....	6
1.8 Literature Review.....	6
1.8.1 Information Security Policy Compliance.....	6

1.8.2 Chatbot.....	8
1.9 User security behaviour.....	11
1.9.1 Factors that influence the behaviour of users.....	15
1.8.2 Non-compliance factors.....	22
1.9.3 Ramifications of non-compliance or poor user security behaviour.....	23
1.9.4 Approaches that encourage compliance.....	24
1.9.5 Acceptable user security behaviour.....	30
1.9.6 How to improve users' security behaviour.....	31
1.10 Research Methodology, Strategy & Design.....	33
1.10.1 Research Methodology.....	33
1.10.2 Research Strategy.....	34
1.10.3 Research Design.....	35
1.11 Data Collection.....	35
1.12 Data Analysis.....	36
1.13 Ethical Consideration.....	37
1.14 Outcomes, Contribution, Significance.....	37
1.14.1 Outcomes.....	37
1.14.2 Contribution.....	37
1.14.3 Significance.....	37
1.15 Summary.....	38
1.16 Thesis overview.....	38

CHAPTER TWO LITERATURE REVIEW.....	39
2.1 Introduction.....	39
2.2 Overview of the field.....	39
2.3 The impact of recognizing compliance and punishing non-compliance.....	40
2.4 Chatbot.....	40
2.4.1 Types of chatbots.....	41
2.4.2 Uses of chatbots.....	42
2.4.3 Key elements of a chatbot.....	44
2.5 Chatbot Framework.....	45
2.6 Chatbots in education and training.....	47
2.7 Chatbot Implementation.....	49
2.8 The gap in the literature.....	51
2.8.1 Introduction.....	51
2.8.2 Method.....	53
2.8.3 Review Protocol.....	53
2.8.4 Research Question.....	53
2.8.5 Search Strategy.....	54
2.8.6 Study Selection.....	54
2.8.7 Inclusion Criteria.....	54
2.8.8 Exclusion Criteria.....	55
2.8.9 Study quality assessment.....	55

2.8.10 Quality Score.....	55
2.8.11 Results.....	55
2.8.12 Data Extraction.....	56
2.8.13 SR Summarization.....	58
2.8.14 Summary.....	61
2.8.15 Limitations and Recommendations.....	62
2.8.16 Conclusion.....	62
2.9 Summary.....	62
CHAPTER THREE: RESEARCH METHODOLOGY.....	63
3.1 Introduction.....	63
3.2 Research Paradigm.....	63
3.3 Research Design.....	64
3.3.1 Experimental Research.....	64
3.3.2 Properties of experimental research.....	64
3.3.3 Ensuring quality in experimental studies.....	65
3.4 Research process.....	66
3.4.1 Experiences.....	67
3.4.2 Motivation.....	67
3.4.3 Literature review analysis.....	68
3.4.4 Hypothesis.....	68
3.4.5 Research Methodology and Strategy.....	69

3.4.6 Conceptual framework.....	73
3.4.7 Data collection.....	74
3.4.8 Data analysis.....	75
3.5 Limitations of the Study.....	76
3.6 Summary.....	77
CHAPTER FOUR: EXPERIMENT PROCESS.....	78
4.1 Introduction.....	78
4.2 Goals of the Experiment.....	78
4.3 Description of the hypothesis.....	78
4.4 Population.....	80
4.5 Population Identification.....	81
4.6 Research Sample Method.....	81
4.7 Instruments that were used in the experiment.....	82
4.8 Tasks.....	84
4.9 Procedures.....	85
4.10 Procedural Analysis.....	86
4.11 Chatbot Architectural Design.....	87
4.12 Protocol Deviation.....	88
4.13 Summary.....	88
CHAPTER FIVE: RESULTS.....	89
5.1 Introduction.....	89

5.2 Descriptive statistics.....	89
5.3 Hypothesis Testing.....	95
5.4 Summary.....	100
CHAPTER SIX: DISCUSSIONS AND IMPLICATIONS.....	101
6.1 Introduction.....	101
6.2 Discussion of results.....	101
6.3 Implications.....	103
6.4 Limitations.....	103
6.5 What the study accomplished.....	103
6.6 Future Research and Recommendations.....	104
6.7 Summary.....	104
REFERENCES.....	105
APPENDICES.....	133
Appendix A: Ethics Approval Letter.....	133
Appendix B: Cyber Security Standards.....	134

LIST OF FIGURES

Figure 1.1: The CIA architecture.....	1
Figure 1.2: The process of testing a hypothesis.....	6
Figure 1.3: Factors that influence user security behaviour.....	8
Figure 1.4: Chatbot processes work.....	8
Figure 1.5: The communication process.....	9
Figure 1.6: Components of a chatbot.....	10
Figure 1.7: Search results in Scopus.....	11
Figure 1.8: Insider behaviour categories.....	13
Figure 1.9: Behavioural security grid.....	17
Figure 1.10: The effect of factors based on the Theory of Planned Behaviour.....	19
Figure 1.11: Illustrates the intersection of security expertise and intention.....	21
Figure 1.12: Non-compliance behaviour types.....	22
Figure 1.13: Information Security Compliance Framework.....	25
Figure 1.14: The Classification of Security Compliant Behaviour.....	29
Figure 1.15: Compliance behaviour.....	32
Figure 1.16: A pictorial representation of the methodological process.....	34
Figure 1.17: Research Strategy.....	35
Figure 2.1: Use Case Diagram of Chatbot Design.....	43
Figure 2.2: Chatbot topic selection based on user's input.....	49
Figure 3.1: Philosophical positivism paradigm.....	64
Figure 3.2: Research process.....	67
Figure 3.3: Conceptual framework.....	74
Figure 4.1: Organisational structure Department 1.....	80
Figure 4.2: Organisational structure Department 2.....	81
Figure 4.3: Two-group simple randomized experimental design.....	82
Figure 4.4: Procedural task analysis.....	87
Figure 5.1: Scatter Chart Experimental Group Department 1.....	90
Figure 5.2: Scatter Chart Control Group Department 1.....	91
Figure 5.3: Bar Chart Experimental Group Department 2.....	91
Figure 5.4: Bar Chart Control Group Department 2.....	92
Figure 5.5: H ₁ Means and Standard Deviations Department 1.....	96
Figure 5.6: H ₁ Means and Standard Deviations Department 2.....	96
Figure 5.7: H ₂ Means and Standard Deviations Department 1.....	97
Figure 5.8: H ₂ Means and Standard Deviations Department 2.....	97

Figure 5.9: H₃ Means and Standard Deviations Department 1.....	98
Figure 5.10: H₃ Means and Standard Deviations Department 2.....	98

LIST OF TABLES

Table 1.1: Chatbot for Organisations and Users.....	10
Table 1.2: User security behaviour categories.....	14
Table 1.3: Insider Types – Matrix.....	15
Table 1.4: Information Security Awareness.....	33
Table 2.1: Comparison of common chatbot frameworks.....	47
Table 2.2: List of studies.....	55
Table 2.3: Quality Evaluation.....	56
Table 2.4: Selection of Primary Studies.....	57
Table 2.5: Delivery Methods.....	58
Table 2.6: Strengths and Weaknesses.....	60
Table 3.1: Characteristics of quantitative research versus qualitative research.....	70
Table 3.2: Comparison of quantitative and qualitative research studies.....	71
Table 3.3: Deductive versus Inductive approach.....	72
Table 3.4: Difference between probability and non-probability sampling techniques.....	73
Table 5.1: Department 1 Demographics data for the sample.....	89
Table 5.2: Department 2 Demographics data for the sample.....	90
Table 5.3: Measures of central tendency and dispersion Experimental group.....	92
Table 5.4: Measures of central tendency and dispersion Control group.....	93
Table 5.5: Measures of central tendency and dispersion experimental group.....	94
Table 5.6: Measures of central tendency and dispersion control group.....	95
Table 6.1: Objectives and Hypotheses.....	101

CHAPTER ONE: INTRODUCTION

1.1 Introduction

In today's digital sphere, awareness and compliance underpin the Information Security Policy's (ISP) success (Flowerday & Tuyikeze, 2016). Hence, the contents of the ISP document should be monitored continuously to have an effective policy. Regardless of how well-designed the organisation's security policies, procedures and guidelines are, security studies do not explicitly explain how employees ought to behave in different security circumstances they experience. Organisations are forced to rely on their employees to execute security resolutions and act as the first line of defence (Häußinger, 2015; Schütz, 2018). The primary goal of information security is to provide *Confidentiality*, *Integrity*, and *Availability*, commonly known as CIA (Kadir et al., 2016). Figure 1.1 depicts the CIA architecture. In order to accomplish the CIA, institutions need to abide by cyber security standards, and these include conducting information risk assessment, threat detection, threat analytics, compliance management, IT auditing, vulnerability assessment, and ensuring that personnel staff are aware of information security policies (Jagtap, Pagar & Meshram, 2018). ISP ensures that users follow information security best practices when using an organisation's information and technology resources (Topa & Karyda, 2016). However, research has shown that users' non-adherence to information security is perceived as a big security concern worldwide (Kolkowska, Karlsson, & Hedström, 2017). This study will focus on compliance management and raising employee information security awareness. Liechti and Sumi (2002) define awareness as being cognisant of the circumstances and the required actions.

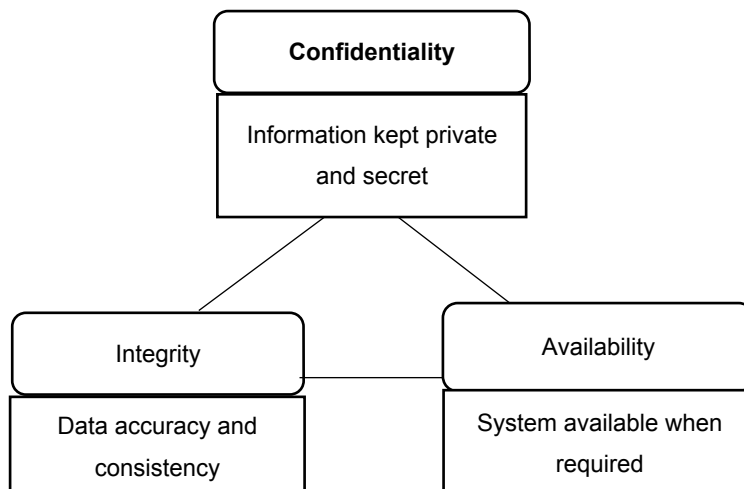


Figure 1.1: The CIA architecture adapted from (Alhassan & Adjei-Quaye, 2017)

Organisations increasingly realize that their staff personnel form an integral part of the business that ought to be well managed and valued; however, despite this, staff personnel still present the greatest cyber security risk (Aldawood & Skinner, 2018). Too often, organisations suffer security harm due to employees who do not abide by ISP. Lack of compliance among employees, either unintended or intended, presents a serious risk to an organisation's information security. Accordingly, much emphasis is needed on promoting values of security awareness and adherence that are directly aligned with an organisation's security policy (Alotaibi, 2017). Globally, non-compliance behaviour toward cyber security is a serious concern that requires urgent attention. Jagtap, Pagar, and Meshram (2018) define Cyber Security as the process of securing devices that communicate in the cyber world against any form of malicious intent that could pose a threat to the organisation and its resources.

Seventy-five percent of large entities and 31 percent of small entities' security violations exploit human vulnerabilities (Omidosu & Ophoff, 2017). These violations include phishing, Bring your Own Device and weak passwords (Ameen et al., 2021). Phishing is a deceptive attempt to gain access to confidential information or access to a victim's device (Peng et al., 2019). Phishing attacks are still extensively used in social engineering; in 2018, 71% of malware distribution groups used spear phishing (Alabdan, 2020). Social engineering is a technique that's used by hackers to trick computer users to gain illegal access to company assets (Krombholz et al., 2015; Aldawood & Skinner, 2020). Phishing emails pose a serious threat every day, thus, affecting major financial institutions and customers (Andronova et al., 2018). Shrestha and Thakur (2019) argue that portable devices offer convenience. However, they are prime targets for malicious programs. Bring your own device, popularly known as BYOD, is at the centre of poor ISP adherence. BYOD allows users to use personal devices to access the organisation's network and resources (Bann, Singh, & Samsudin, 2015). Aguboshim and Udobi (2019) believe that over 50% of IS transgressions can be linked to portable instruments. Research has shown that users often ignore the risk associated with weak passwords (Yildirim & Mackie, 2019).

1.2 Background to the study

Information system (IS) users make decisions that can impact the whole business entity, both positively and negatively. Organisational leaders need to ensure that the employees are well

equipped to understand and recognize their role towards the security of the organisation. However, due to the complexity of security measures often placed around information systems, users will always look for ways to bypass information security controls (Harrell, 2014; Mahfuth, 2019). According to Haingura (2019), the human factor in information security refers to employee actions that can lead to a breach in IS. These actions result from poor security conduct, negative attitude towards ISP, unhappy users, theft, and insufficient knowledge. Haingura (2019) further notes that technical controls include firewalls, intrusion detection systems, and Data Encryption Standards (DES). These controls aim to protect organisations against hacking, viruses, and software piracy.

The insecure circumvention of security controls can be attributed to many factors. Users do not adopt available and accessible information security measures, which renders technical controls less effective (Omidosu & Ophoff, 2017). Studies past and present suggest that authorization contributes to the circumvention of security controls, and users look for cheaper ways of accomplishing their daily tasks (Bartsch & Sasse, 2012; Yaokumah & Kumah, 2018). For instance, if a policy change is cumbersome, users would instead share resources, albeit the policy states clearly that resources such as passwords should not be shared at all (Mahfuth, 2019). Employees' negative attitudes and poor conduct towards security controls compromise the IS. Employees must appreciate the importance of security controls and their value in promoting cyber-security (Haingura, 2019). Security teams still face a significant challenge in enhancing ISP compliance (Topa & Karyda, 2016). In the current literature, Lowry (2017), Liu, Wang and Liang (2020) have discussed the issue of end-user compliance at length, and different approaches to improving ISP compliance have been suggested. However, based on the current literature, there appears to be a gap in the extant literature regarding ensuring ongoing ISP compliance.

1.3 The Role of Chatbots in End User Security Compliance

Chatbots have become dominant in various fields, industries and education (Winkler & Söllner, 2018). According to Nair and Johnson (2018), chatbot applications are now regarded as modern-day browsers. Chatbot technology is perceived as the future of communication between humans, webpages, and applications. MITTechnology has listed chatbots among the top 10 technology discoveries of 2016 (Dale, 2016). This view is still supported by current

literature by Fryer and Nakao (2019); Chaves and Gerosa (2021). A chatbot responds using the same applications, creating a back-and-forth conversation (Caldarini, Jaf & McGarry, 2022). The use of chatbots will help enforce compliance and raise awareness at the same time. Further to this, the term chatbot dates back to the Nineties. It implies a computer program that intends to simulate and reproduce a smart interaction with a user (Adamopoulou & Moussiades, 2020). Chatbots are sometimes referred to as conversational agents due to their ability to allow two-way communication with users through the use of human language. Communication can be text or vocal-based. In the latter case, a chatbot is also referred to as a voicebot (Pigliacelli, 2020). The ease of use of chatbots gives a significant benefit to using a chatbot for users. Chatbots are instant messaging applications (Dahiya, 2017).

Additionally, chatbots offer easily understandable conversations, resulting in a positive and engaging user experience. Unlike conventional communication avenues, such as telephone and email, chatbots offer a prompt and dependable service that ensures swift and convenient replies to various queries (Varitimiadis et al., 2020). Considering that chatbots are capable of handling large volumes of data and users, chatbots can act as assistance service operators (Barricelli et al., 2018). Some studies have been conducted on Information Security Awareness and User Compliance (e.g., Harrell, 2014; Kadir et al., 2016; Alotaibi, Furnell, & Clarke, 2017; Kolkowska, Karlsson & Hedström, 2017). However, there seems to be insufficient research on enforcing user compliance using a chatbot. Using a chatbot will not replace authentication, authorization and accounting services. Thus, a chatbot will not authenticate users or authorize users' access and track the user's activity. Also, a chatbot will not replace information security awareness and training. Instead, a chatbot will provide auxiliary aid to users' compliance and ensure that the contents of ISP are carried out incessantly. Therefore, a chatbot will constantly remind users about the contents of the information security policy and ensure ongoing compliance. Henceforth, chatbot use will be limited to password policy, bring your own device, or removable media policy and phishing.

1.4 Problem Statement

Employees' non-compliant tendencies towards information security policies have become an enduring concern. Current information security analysis approaches fail to provide information security managers with enough information to capture the reasons that influence users'

compliance and non-compliance (Kolkowska et al., 2017). Currently, users' compliance behaviour shows no sign of improvement after attending security awareness and training. This lack of compliance can have unwanted ramifications on the organisation's resources and lead to financial cost, loss of valuable time, and in most cases, compromise of the organisation's security. A breach in an information system can have severe repercussions for an organisation. Rao et al. (2020) points out that a data breach is likely to have a potential economic impact, market value impact and customer trust impact. Fischer (2015); Sarker et al. (2020) argue that a cyber-breach can have a harmful impact on the confidentiality, integrity, and availability of an ICT system and the information it stores. Cybercrime or cyber-spying can result in financial, proprietary, or personal information loss, from which the attacker can benefit; often, the target is unaware of these malicious activities (Stanciu & Tinca, 2017; Wang & Wang, 2019). Based on the issues raised thus far, the study believes that a chatbot could be useful in enforcing compliance and reducing potential data breaches among ICT users.

1.5 Research Aim

This study aims to determine the impact of a chatbot in enforcing ongoing user compliance in selected government entities.

1.6 Objectives

The objective of this study is to use a prototype model (e.g., chatbot) to enforce compliance and raise awareness in selected government entities. The study will attempt to:

- a) Conduct the experiment using a chatbot as a treatment; and
- b) Ascertain whether the use of chatbots can improve ISP compliance.

1.7 Hypothesis

Independent variable X: Policies [strong password, attachments, and scan devices].

Dependent variable Y: Compliance factors [Compliance, Non-Compliance].

1.7.1 Educated Guess

The hypothesis for this research study is that users who receive a constant reminder about the contents of ISP have a higher information security compliance behaviour than users without any form of reminder.

1.7.2 Null Hypotheses H_0

There is no relation between using strong passwords, spotting phishing attachments, scanning portable devices and using chatbots.

1.7.3 Alternative Hypotheses

H_1 : There is a positive relationship between improved user password compliance behaviour and the use of chatbots.

H_2 : There is a strong relationship between users' ability to spot a phish and the use of chatbot

H_3 : There is a positive relationship between users who scan their portable devices before they use them on the company network and the use of chatbots. Figure 1.2 depicts the process of testing a hypothesis.

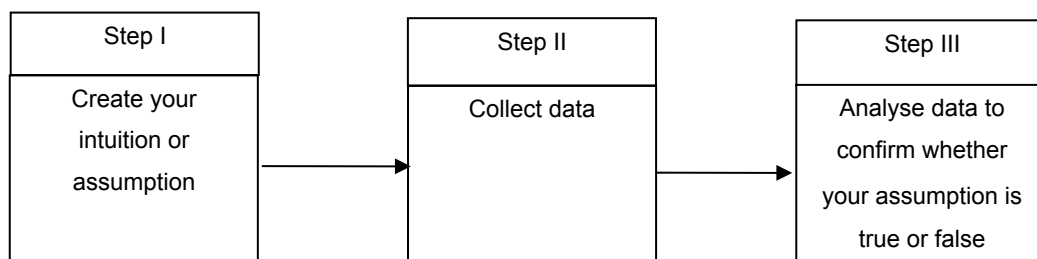


Figure 1.2: The process of testing a hypothesis adapted from (Kumar 2011)

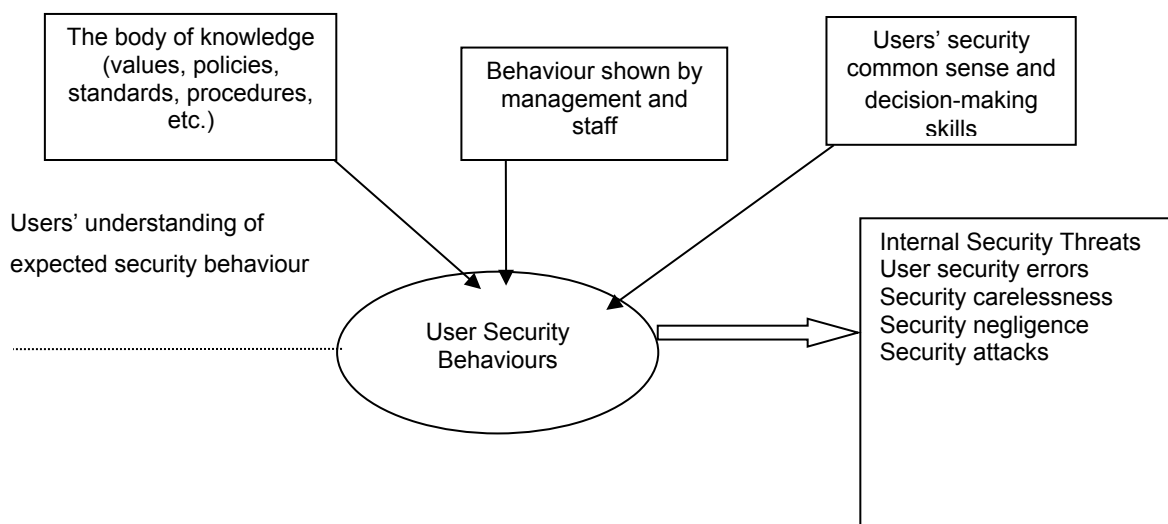
1.8 Literature Review

1.8.1 Information Security Policy Compliance

Previous studies on cyber security have consistently proved that Information Security Policy is key to user compliance. The ISP outlines acceptable and unacceptable user behaviour (AI-

Omari et al., 2013; Alotaibi, 2019). Alotaibi et al. (2017) asserted that some researchers have tried to pinpoint the key factors behind varying degrees of compliance with information security policy. Academic literature and information security institutes' reports on information security policy compliance have been reviewed in this regard. The influencing factors have been categorised into two types, namely, organisational and human. Organisational factors that affect human behaviour are Information (i) Quality (Data flow), (ii) Motivation and Sanction (Deterrence), (iii) Awareness and Training, (iv) Computer Monitoring and Persuasion and User behaviour are influenced by: Perception (Situation Awareness), Personality, Technology democracy, Cultural factors, Gender, Satisfaction and Habits (Alotaibi, Furnell & Clarke, 2016).

Similarly, Goode et al. (2018) highlighted the crucial role of Information Security Awareness in Information Security Policy Compliance. In their view, employees should be able to detect (awareness) security threats and demonstrate a degree of knowledge about information security and be up to date or stay abreast with security technology and clearly understand what it is all about. This definition is in line with the notion that information security awareness (ISA) refers to a state where employees in a business entity are cognizant of and ideally have a buy-in to the security mission. Therefore, organisations require their employees to possess basic knowledge and awareness of security issues, which should be reflected in their daily operations and interactions with ISPs (Khan & Alshare, 2019). In addition, Hina and Dominic (2017) recommend that ISA and training programs have an essential part to play in adopting protective technologies, developing a security culture, and compliance with organisational policies. Adaptable awareness programs can be tailored to enhance the ever-evolving organisational security demands (Alotaibi, 2019). Sherly and Lifang (2015); Javidi and Sheybani (2018) believe that users' security behaviour is impacted by various factors, as depicted in figure 1.3, which shows factors that influence user behaviour.



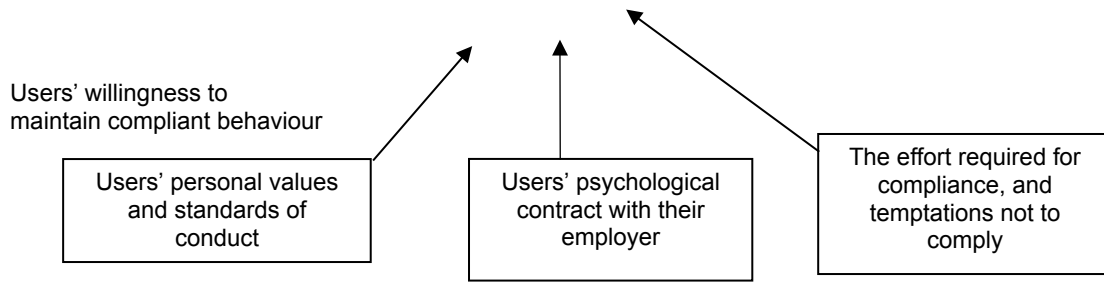


Figure 1.3: Factors that influence user security behaviour adapted from (Sherly, 2011)

1.8.2 Chatbot

Recently, the proliferation of chatbot use has significantly propelled artificial intelligence (Berge, 2018). In figure 1.4, a user queries a chatbot, and then a chatbot performs a series of tasks that generate a response to the user's query. Figure 1.4 illustrates how a chatbot process works.

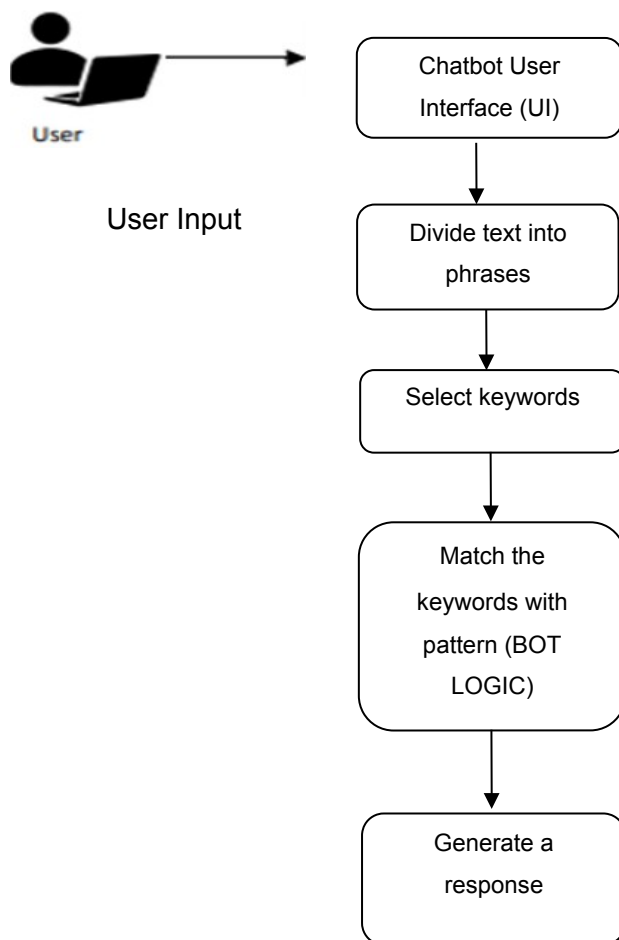


Figure 1.4: Chatbot processes work adapted from (Al-Omari et al., 2012)

The use of chatbots in the training and education sphere is gaining momentum. Villegas-Ch, Arias-Navarrete and Palacios-Pacheco (2020) argue that chatbots have significantly influenced learner interactions with information and content. This ability puts chatbots at the centre of these interactions in online learning environments. Meyer von Wolff, Hobert and Schumann (2019) add that chatbots should assist users during the onboarding process by providing answers to corresponding queries and assisting users in learning company specifics. Additionally, lifelong learning at work can be achieved through the use of chatbots. Positive conduct of users has been noted in areas where chatbot use is adopted to conduct security education (Gulenko, 2014; Majumder & Mondal, 2021). Figure 1.5 depicts the communication process of a chatbot from the user input (sender) to generating feedback (recipient).

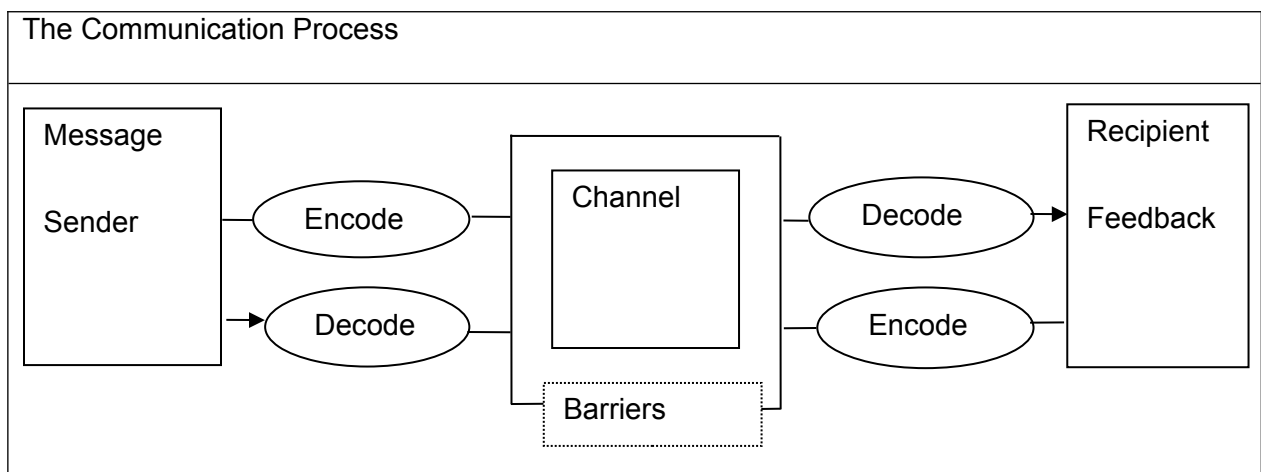


Figure 1.5: The communication process adapted from (Oduntan & Adegboye, 2017)

Meyer von Wolff et al. (2019) noted that a chatbot's structural design comprises compulsory and optional components (see figure 1.6). The optional components include input options, i.e., voice or text. Mandatory components are automatic speech recognition and natural language understanding. Their role is to ensure that the input is in the format that a machine can understand and to divide the input into small groups of lines. The dialogue manager is an intermediary between the natural language processes and the backend.

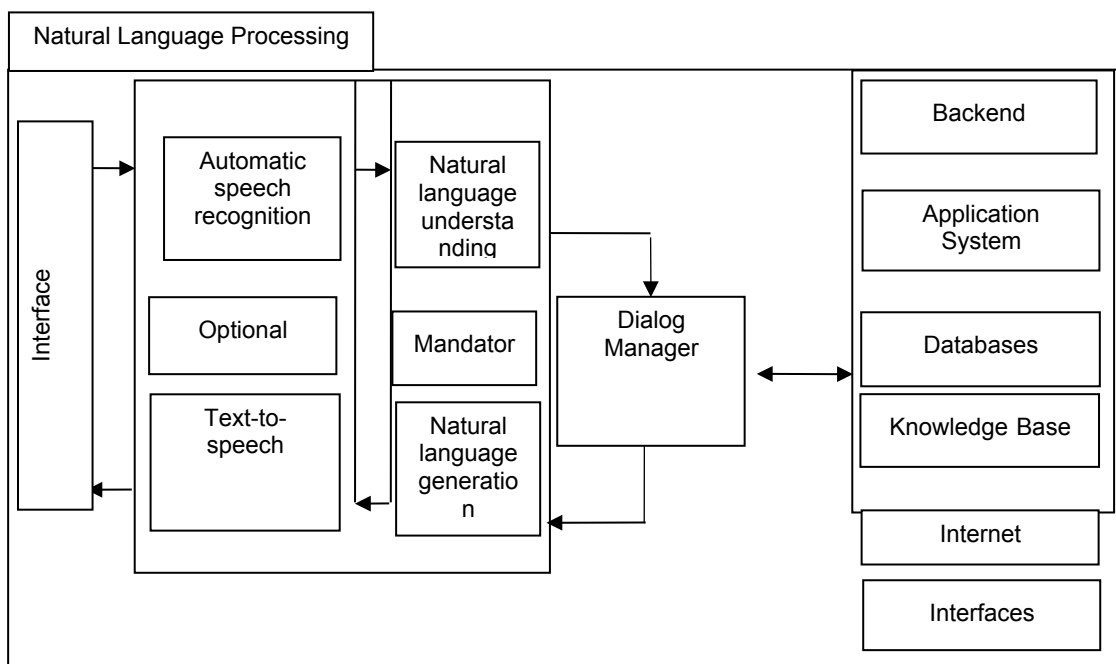


Figure 1.6: Components of a chatbot adapted from (Meyer von Wolff et al., 2019)

Table 1.1 tabulates the benefits of using a chatbot for organisations and users. Zumstein and Hundertmark (2018a) list the following chatbot benefits:

Table 1.1: Chatbot for Organisations and Users adapted from (Zumstein and Hundertmark 2018a)

Organisations	Users
Available 24/7	Customer service and support are available

	24/7
New and direct customer points	One-to-one communication on a personal device
New methods and types of data collection	Convenient and easy to use
A high amount of personal user or usage data	Time and cost saving
Personalization and automation of information	Reduction of relevant information and services
Reduction of service and support cost	Customized options relevant to user(s) preferences

Figure 1.7 shows chatbots' exponential rise, particularly after 2016. The diagram explains how chatbot popularity has grown exponentially and how often the keyword(s) chatbot, conversation agent, or conversational interface was searched from 2000 until 2019. This diagram highlights the importance of chatbots in future learning, and particularly in this study, a chatbot will add value to IS awareness and training and complement conventional training methods.

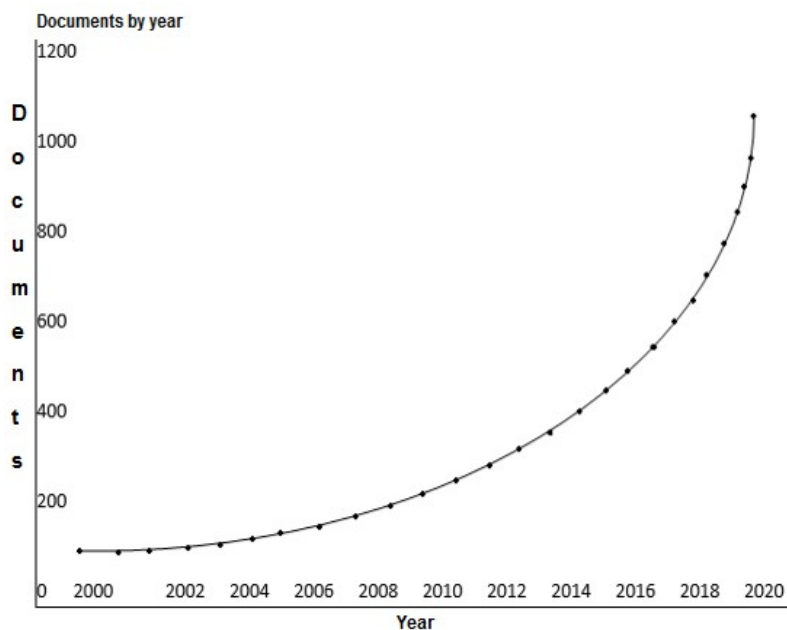


Figure 1.7: Search results in Scopus adapted from (Adamopoulou & Moussiades, 2020)

1.9 User security behaviour

Organisational security behaviour, or security hygiene, is the set of information regarding data protection expectations that a company places on the end-user as part of security practice (Banfield, 2016). Organisations adopt information security policies with awareness campaigns, training, incentive schemes and disciplinary procedures, primarily to govern and improve the conduct of users, promote information security awareness, maintain a coherent adherence to information security policy and, above all, secure information resources. (Shen, 2016). Chang and Lin (2015); Da Veiga and Martins (2017) reckon that information security policy has several key aspects in realizing the ultimate information security goal. However, human behaviour is one aspect of information security policy that organisations find difficult to manage. Adding to the challenges around human behaviour control is the difficulty of evaluating and monitoring human behaviour. Consequently, security awareness relies heavily on self-reported questionnaires and surveying users using this same instrument (Al Salek, 2021). The effectiveness and validity of this approach are virtually impossible to determine. Instead, organisations hope that exposure to security training and awareness will influence the behaviour of employees (Fertig & Schütz, 2020).

Studies have tried to analyse how humans make security decisions (Egelman & Peer, 2015; Egelman, Harbach & Peer, 2016; Gratian et al., 2018). Shillair and Meng (2017) are of the view that users' level of knowledge and skill play a pivotal role in influencing users' security conduct, user's ability to take appropriate security decisions depends on the user's security awareness and understanding, and thus, users who lack security awareness and understanding are always sceptical about their security capabilities. However, users base the decision to be compliant or defiant on what needs to be achieved, how they perceive security, attitudes and norms (Kirlappos, Parkin, & Sasse, 2014; Dang-Pham, Pittayachawan & Bruno, 2017). On the contrary, Ngoqo and Flowerday (2015); Sarker et al. (2020) observed that where users demonstrate high levels of security knowledge, the standpoint toward information security tends to be positive.

Furthermore, it is stated that there are two distinguishable sets of end-user behaviours that positively affect security: cyber hygiene and threat response (Maennel, Mäses & Maennel, 2018). Cyber hygiene is proactive in its approach to reducing security breaches. Scanning a computer for viruses, backing up data, and updating and using strong passwords are typical

examples of cyber hygiene behaviours. On the other hand, threat response is reactive and requires users to respond or react to any potential threat and detect and prevent potential threats from materializing. Scanning a computer after a malware alert or any strange or abnormal computer activity, not visiting websites deemed not secure and performing system updates and upgrades to thwart a breach are part of threat response behaviour (Kelley, 2018).

In addition, Warkentin and Baskerville (2013); Menard, Bott and Crossler (2017) argue that insider threats that can directly or indirectly impact the organisation’s system resources can be grouped into two classifications: deviant behaviours and misbehaviours. Users with malicious intent are usually branded as having deviant behaviours. Such users are capable of sabotage, stealing and industrial or political espionage. Warkentin and Baskerville (2013); Safa, Von Solms and Furnell (2016) further state that users with no malicious intent are usually called misbehaviours. Such users create weak passwords, visit non-work-related websites using corporate computers, accidentally post confidential data onto unsecured servers or websites or unwittingly click on phishing links on emails and websites (Menard et al.,2017).

Insider behaviour can be malicious, neutral, or benevolent. Malicious intent is intentional and detrimental. Neutral behaviour can be dangerous and prone to mistakes, whereas benevolent behaviour is obedient and intends to protect the organisation against malicious attacks (Djajadikerta, Mat Roni & Trireksani, 2015; Ali et al., 2021). Figure 1.8 illustrates the insider behaviour categories.

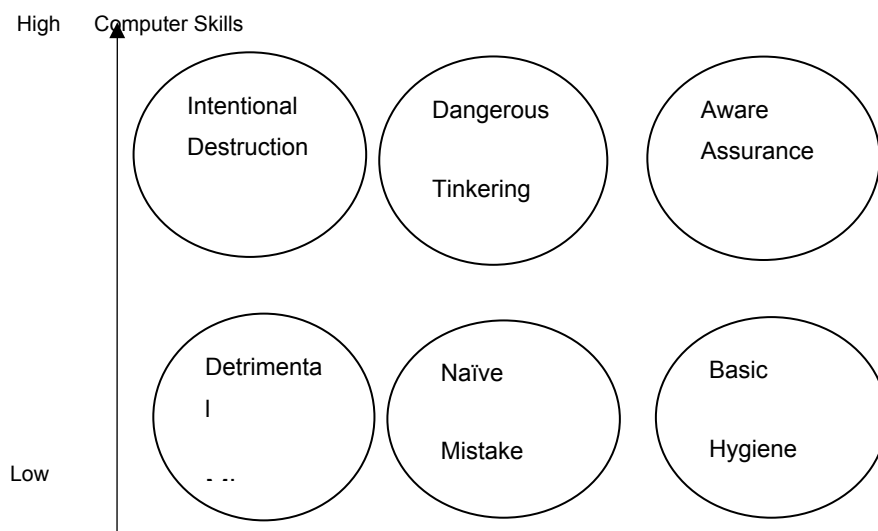




Figure 1.8: Insider behaviour categories adapted from (Djadjdikerta, Mat Roni & Trireksani, 2015)

Table 1.2 provides a summarized description of the six categories of behaviour that are associated with insider behaviour.

Table 1.2: User security behaviour categories adapted from (Ngoqo & Flowerday, 2015)

Awareness	Intention	Behaviour	Description
High	Low	Destructive	Behaviour is associated with high levels of awareness and desire to be compliant
Low	Low	Detrimental Misuse	This user behaviour has minimal levels of awareness, but it is prone to compliant behaviour
High	Neutral	Dangerous Tinkering	This behaviour requires high levels of awareness with a strong desire to remain compliant
Low	Neutral	Innocent Mistake	This behaviour is associated with minimal levels of awareness and no desire to engage in non-compliant behaviour
High	High	Aware Assurance	High levels of awareness are required, and the intent to be compliant is evident
Low	High	Basic Hygiene	Low levels of compliance are required with apparent intent to uphold compliant conduct

User threat models usually determine the sophistication of their technical models. Some factors contributing to users' security apathy are not feeling personally targeted, naivety or believing imposters (like companies or government), and accepting their existing mitigation strategies to be sufficient (Zeng, Mare, & Roesner, 2017). Therefore, promoting secure online behaviour and ensuring proper security conduct remains challenging due to users' mindsets and how they interpret risk. According to Yan, Xue and Lou (2021), the casual behaviour of some users towards cybersecurity shows is a source of major concern. Users undermine security measures and believe the chances of getting attacked are next to zero. Users come up with questions like, "Why would we have to be so uptight about cybersecurity? Who would want to attack our institution out in the middle of nowhere?" (Richardson et al., 2020).

Furthermore, Safa et al. (2015); Chenthara et al. (2019) noted that employees' view of security depends on how cyber incidents are handled. When users find it difficult to apply security recommendations, they might fail to interpret and trust them and subsequently bypass security measures. Another contributing factor, according to Balozian and Leidner (2017), is negligent insiders. Negligent insiders can be categorized based on their ability and willingness, i.e., some IS users are willing to adhere to the security policies but are unable due to (naïve acts that are due to lack of awareness or training). In contrast, other users can comply but have no desire to comply (opportunistic acts that can be attributed to negative motivation). The only differentiating factor between these two negligent subgroups and malicious insiders is that the two subgroups have no malicious intent toward the organisation (see table 1.3). Consequently, the two subgroups (naïve acts and opportunistic acts) are treated as negligent insiders. Naïve and opportunistic users are noncompliant. However, they do not have malicious intentions. The malicious intent group is regarded as defiant and does not desire to adhere to IS policies. Their lack of compliance is deliberate and is driven by malicious intentions toward the organisation (Balozian, Leidner & Warkentin, M., 2019).

Table 1.3: Insider Types – Matrix adapted from (Balozian & Leidner, 2017)

Intent	Ability	Desire to comply	Resultant	Resultant Behaviour
--------	---------	------------------	-----------	---------------------

			Behaviour of Compliance	of Non-compliance
Malicious	High Expertise	Willing to comply	Compliant	Malicious
Non-malicious	Low Expertise	Unwilling to comply	Negligent and naive	Malicious Threatening

1.9.1 Factors that influence the behaviour of users

The motive behind users' deliberate misconduct is driven by profit or destruction. These types of users are often called intentional malicious insiders (Banfield, 2016). The users whose intentions are not to harm the organisation but still inadvertently fail to comply and demonstrate conduct that compromises the organisation's security or exposes security resources are often labelled as unintentional insider threats. Emotions and the environment distinguish whether a user's conduct is based on intentions or behaviour (Wash & Rader, 2019). The failure of users to practice cyber hygiene behaviours is due to the absence of knowledge about the significance of hygiene conduct and what it means to the user and the organisation (Kelley, 2018). In addition, Blackwood-brown (2018) argues that risk in security tends to be subjective, meaning a user's perception of risk significantly influences the user's security stance. Thus, cybersecurity risks do not receive the necessary attention. Users can become less appreciative of security controls and processes, particularly if they view them as a stumbling block hindering them from accomplishing their primary function. (Bada, Sasse & Nurse, 2019).

An increasing trend shows users' failure to abide by the security policies because users find security policies onerous (Alghamdi, Win & Vlahu-Gjorgievska, 2020). The rationale behind this increasing trend is that, in most cases, the policy documents contain information irrelevant to the users and security threats that will not directly impact the users. Thus, users perceive compliance as a waste of time (Simpson, 2019). Blum (2020) posits that management needs to streamline and implement policies that would benefit the organisation and avoid perceiving IS policies as wasting users' time. Getting users to buy into the entire security policy is somewhat challenging because different users are affected by various aspects of information security. Pinpointing what is relevant to each set of users should be the starting point of security awareness and enforcement. If initial training is centred on the most pertinent aspects of security, users will have no problem adopting IS policy.

According to Kirlappos et al. (2014); Dang-Pham, Pittayachawan and Bruno (2017), factors that lead to adopting non-compliant behaviours are:

Lack of awareness: If users lack security awareness and are oblivious to the implications of non-compliance, then users will not be motivated to uphold acceptable security conduct.

High compliance costs: When security compliance competes with production, employees will not allow production to suffer because a pending security compliance task must be completed.

Compliance impossible: If the employees find the recommended security solution(s) onerous, employees will find ways to bypass the security controls to perform their major function (Nicholson, Coventry & Briggs, 2019).

Security behaviour conforms to the Johari window quadrants (Open, Hidden, Blind and Unknown), enabling companies a simple heuristic to classify behaviour (see Figure 1.9) (Beris et al., 2011; Maennel, Mäses & Maennel 2018). All the employees that conform to the security conduct and whose behaviour is in line with security policy and security-related risks would fall into the (Open quadrant). These employees have shown general knowledge and are aware of the risks associated with security. Moreover, these users know what is required, and their outlook on security matters is constructive (Flowerday & Tuyikeze, 2016). Clary (2014); Gandy-Guedes et al. (2016) posit that in the (Blind quadrant) the user is unaware of what type of information is being disclosed on public platforms and is oblivious to how this information is received or exploited. Hidden quadrant users know they are expected to behave in a compliant manner, but they choose to hide or not uphold this compliant conduct (Sveen, 2016). Employees in the (Unknown quadrant) have no faith in the organisation's security; they believe security methods are inferior, and employees are unaware of the security risks the organisation faces. Therefore, this results in a limited amount of employees who know the security risks that affect the organisation. A solution to this problem is to point out unknown threats impacting the organisation and address them accordingly (Beris et al., 2011; Heartfield et al., 2018).

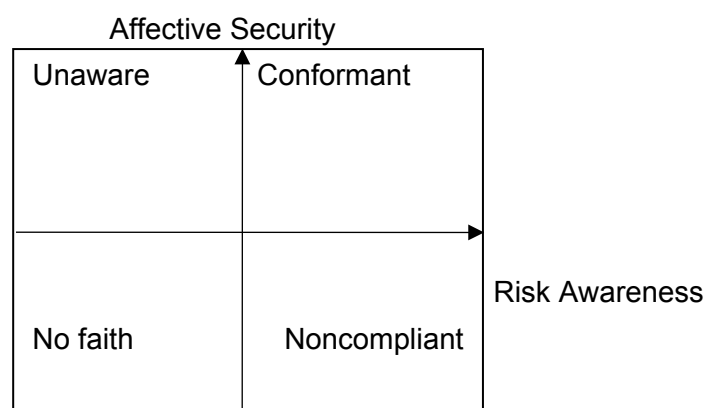


Figure 1.9: Behavioural security grid adapted from (Beris et al., 2011)

Egelman, Harbach and Peer (2016) have proposed a Security Behaviour Intentions Scale (SeBIS) method that evaluates user's self-reported intent to comply with "good" security practices around the following four dimensions:

1. *Awareness*: Are the users aware of contextual hints, such as the web browser URL bar or various security iconography?
2. *Passwords*: Do users' passwords conform to the password policy, that is, the password is not easily predictable, and it meets the password length?
3. *Updating*: Do users run software updates and scan their devices for viruses?
4. *Securement*: Do users ensure that security is enabled on their devices with secret codes, such as using smartphone secure lock screens (i.e., requiring a PIN) or password-protected screen savers on desktops and laptops?

The three types of beliefs that influence a user's conduct are behavioural, normative, and control beliefs (Kim & Kim, 2020). Behavioural beliefs are often associated with good or bad behaviour concerning the user's conduct and touch on a positive and negative assessment of behaviour (Safa et al., 2016). Haingura (2019) points out that normative beliefs influence subjective norms, that is, how a user perceives other users' conduct regarding information security. Gerstorf et al. (2019) posit that control belief or perceived behavioural controls refer to the user's ability to attain the desired end result. Kim and Kim (2020) note that perceived behavioural controls may positively or negatively impact behaviour performance by limiting or supplying resources such as budget, training and knowledge to users. Similarly, an individual's perspective on security is conceived during compliance-related repercussions that affect compliance (effort, time) or non-compliance (punishment) with the ISP (Bulgurcu et al., 2014; Simonet & Teufel, 2019).

Cost-benefit assessment of compliance and non-compliance greatly affects how users perceive ISP compliance and what it intends to achieve (Ifinedo & Akinnuwesi, 2014; Young et al., 2017). In addition, security culture, job satisfaction and perceived organisational support all positively contribute towards security compliance objectives (Cheng et al., 2013; Cram, Proudfoot & D'arcy, 2017). Rupere and Muhonde (2012); Algarni, Almesalm, and Syed (2018) note that an individual's behavioural commitment is influenced by the risk assessment associated with various possibilities. In most cases, risks related to information security are naturally accumulative. There is also optimism bias, whereby users believe they are less likely to experience any security threat. These people believe the likelihood of any risk occurring to them is too low compared to others. Optimism bias is especially pervasive in information security. Research has shown that, in many instances, users do not regard the information stored on their devices as valuable to hackers. As such, they do not see themselves as possible cyber prey (Hewitt & White, 2022).

Das et al. (2014); Fagan et al. (2017) point out that group standards or rules can override the individual's security conduct. People tend to align their individual behaviour with the group's behaviour. If the entire group can see value in information security, then probably, the individual members of the group will treat information security with respect and adherence. Contrarily, if the group encourages risk-taking, it is highly possible that individuals will venture into more risky exploits. Figure 1.10 depicts the theory of planned behaviour (TPB). According to Safa et al. (2015); Safa et al. (2019), TPB explains the effect of attitude, subjective norms, and perceived behavioural control on individual behaviour.

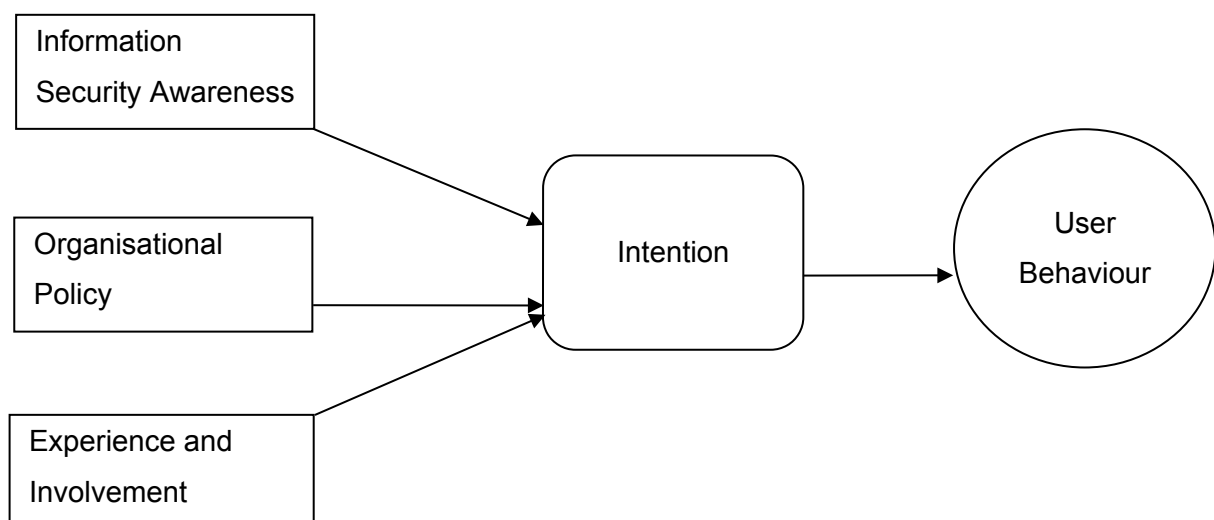


Figure 1.10: The effect of factors based on the Theory of Planned Behaviour adapted from (Safa et al., 2015)

Furthermore, users' perception of security threats is influenced by the likelihood of the threat happening and the impact associated with the perceived threat (Donalds & Osei-Bryson, 2020). Some end-users do not follow security best practices and conduct (Wynn et al., 2013; Hameed & Arachchilage, 2020). Similarly, Gratian et al. (2018) believe that cybersecurity behaviour and the four major categories of individual differences: demographic factors, personality traits, risk-taking preferences, and decision-making styles, are indeed interlinked. Demographics can include various elements in a human population, e.g., age, gender, role, major, citizenship, and employment length at the university. Personality traits refer to individuals' disposition characteristics of agreeableness, conscientiousness, neuroticism, openness and extraversion will significantly correlate with their security behaviour intentions of device securement, password generation, proactive awareness, and updating.

Risk-taking preferences of individuals' urge to venture into risky adventures will significantly correlate with their security conduct objectives of device securement, password generation, proactive awareness, and updating. Decision-making styles refer to the individuals' ability to make a decision that will significantly correlate with their security conduct and intents of device securement, password generation, proactive awareness, and updating.

Users' conduct can be affected by limited security awareness and paucity of motivation and knowledge (Acquisti et al., 2017). Many end-users are unaware of the security pitfalls and what resources can help them ward off them. In some cases, users are aware of security resources at their disposal, but due to the absence of motivation, they fail to protect themselves and the organisation (Rader & Wash, 2015; Wash, Nthala & Rader, 2021). Simplifying security tools can help improve compliance. In some instances, users have the awareness and desire to comply. Still, users become demotivated due to the complexity of security processes and limited knowledge to apply security principles (Das et al., 2014; Nicholson et al., 2019). In addition, Wash and Rader (2019) observe that demographic differences influence security beliefs and conduct. Semi-literate users are more likely to believe that devices can be infected by simply viewing web pages and that there are no measures that can help them prevent cyber-attacks.

Similarly, people with less than a high school degree are also likely to be vulnerable to cyber-attacks and hacking because they are most likely not to follow any preventive measures (Fulton et al., 2019). People with lower levels of basic education are more exposed to cyber-attacks because they do not know where to find help and what protective measures they can take (Nicholson et al., 2019). Older people would be less likely to believe that simply surfing the internet can infect your device with malware. Also, educated people would find it hard to believe that cyber-attacks prey on home users. Older people and people with a high school education or greater tend to be more cautious and adopt preventive measures. These users think they are capable of protecting themselves. However, they usually do not believe hackers would target them (Wash, Nthala & Rader, 2021).

Even though companies ensure that employees receive the appropriate training in proper security hygiene conduct and are equipped with necessary security tools, users do not fully embrace security policies. In the long run, they stop practising proper security conduct for various reasons. Research has shown that users can only continue with compliance if there is a perceived threat (Vedadi & Warkentin, 2018). Once the suspected threat disappears, users automatically drop their guard and forget about security risks. Once the immediate threat has been dealt with, users see no reason to apply preventive measures. Research points out that users take compliance seriously only when the users or the company are exposed to a specific cyber threat (Anderson, Abiodun & Christoffels, 2020). If there are no noticeable risks, users will no longer continue to maintain proper security conduct. It is also said that users do not embrace new security methods until they can ascertain their efficiency (Warkentin et al., 2016). Users' counterproductive computer security behaviour (CCSB) is influenced by various factors (Hadlington, Binder & Stanulewicz, 2021). These factors include locations or contexts and particularly socioeconomic factors (i.e., national wealth (GDP), transparency, and literacy rates), and the cultural dimensions of individualism versus collectivism (IDV) and uncertainty avoidance (UAI) reviewed in this study were found to have noteworthy significance on participants' desire to indulge in CCSB at work. (Ifinedo & Akinnuwesi, 2014; Ifinedo, Longe & Amaunam, 2017). Alghamdi et al. (2020) believe that companies do not provide users with adequate training or they do not enforce compliance. For instance, in many organisations, users still fall for phishing scams and continue to open email attachments intended to infect their devices with malware. Employees continue to lose devices that have important and classified data. Alkalbani, Deng & Zhang (2016) argue that users' fear of being punished for

non-compliance with ISP contributes significantly to their behaviour and perception of ISP. Figure 1.11 illustrates the intersection of security expertise and intention.

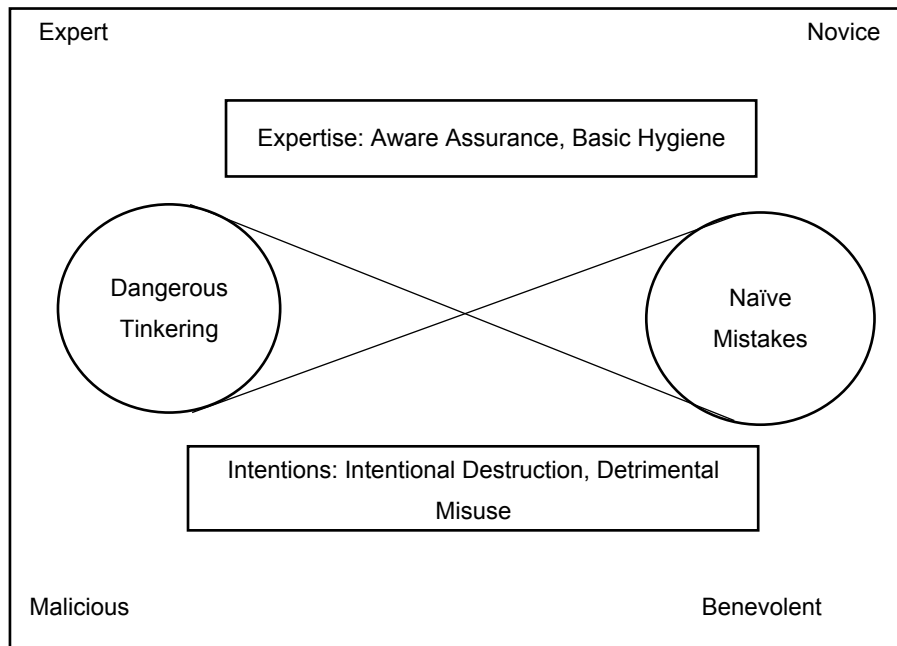


Figure 1.11: Illustrates the intersection of security expertise and intention adapted from (Banfield, 2016)

1.8.2 Non-compliance factors

The key elements that impact ISP compliance are security risk evaluation and cost of compliance from the protection motivation theory. Studies have found that the demands of compliance placed on employees have proved to be a huge hindrance to user compliance (Pham, El-Den & Richardson, 2016; Gangire, Veiga, & Herselman, 2019). Additionally, the convolution, lack of clarity, and amount of work associated with security compliance are some issues that negatively impact security adherence. It is said that these issues increase stress levels for employees and morally detach employees from security activities. In a nutshell, security compliance hinges upon what is required from the user versus what the user can deduce from security activities (Pham et al., 2017). Humaidi and Balakrishnan (2018) recommend that the contents of ISP must be intelligible and delivered in a simplified manner so that users can identify with security recommendations and embrace ISP compliance.

The inability of users to discern the risks of non-compliance behaviour poses a serious threat and negative ramifications on user compliance (Charlette, 2015; Donalds & Osei-Bryson, 2020). Further, Alotaibi (2019) states that non-compliance with ISP has two main categories, intentional and unintentional. Intentional non-compliance conduct includes deliberate methods with the sole intention of disrupting security processes and inappropriate uses of security resources. The motive behind this act of malice is to ruin the institution. Unintentional non-compliance conduct is a resultant lack of awareness or sometimes negligence. Figure 1.12 describes types of non-compliance behaviour.

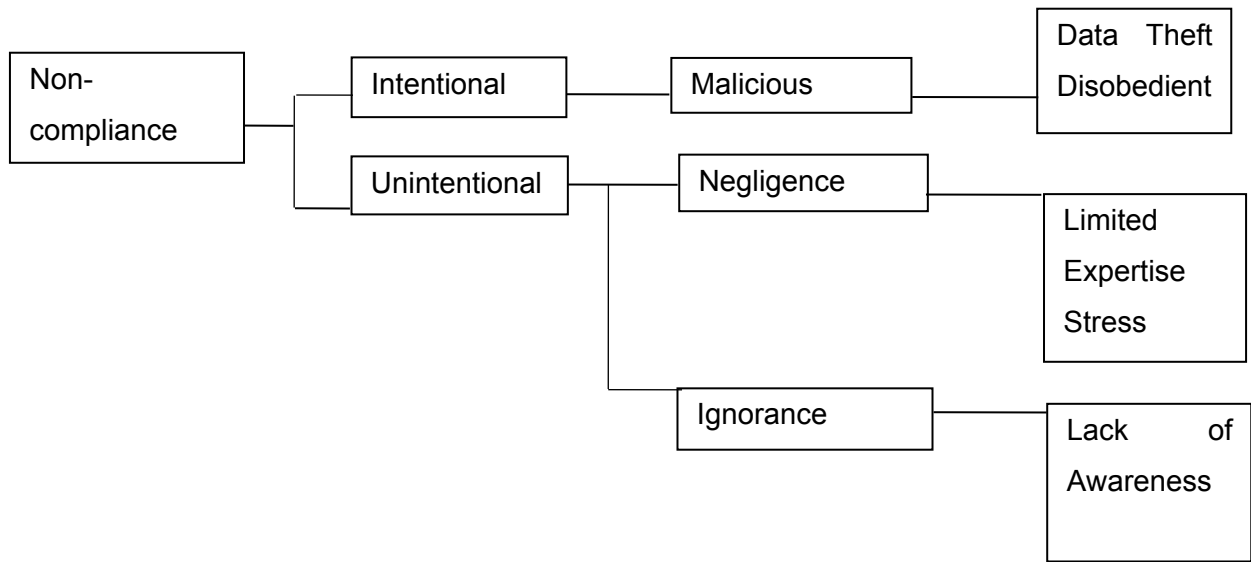


Figure 1.12: Non-compliance behaviour types adapted from (Alotaibi, 2019)

A combination of organisational and personal determinants can play a huge role in how users relate to security requirements (Pham et al., 2017). Information security manuals or web pages are generally tedious, with a list of what to do and what not to do. On top of that, the impact of the ISP documents on users' security behaviour is minimal because users only get to view the documents when they have to perform their yearly security training and compliance (Kirlappos et al., Rajas 2013; Kolkowska et al., 2017). Institutions inadvertently contribute to the high rate of non-compliance. They do not have a balance between production and security. Employees are expected to meet their primary targets and still find time to worry about security matters (ibid 2013). Often users are compelled to choose between their major function and security compliance. Intuitively users choose their major function because of the benefits associated with their key job function (Kirlappos, Parkin & Sasse, 2014; Zimmermann & Renaud, 2019).

1.9.3 Ramifications of non-compliance or poor user security behaviour

Failure to abide by information security policies will lead to the inefficacy of information security methods (Alghamdi et al., 2020). Organisations could face unwanted ramifications if compliance is not enforced, including corporate liability, loss of credibility, and monetary damage (Bulgurcu et al., 2014; Sanders, Upadhyaya & Wang, 2019). Kirlappos, Beutement and Sasse (2013); Karlsson, Hedström, and Goldkuhl (2017) advise that companies need to encourage compliance to avoid dealing with perennial information security risks. Intellectual property theft can negatively affect competitiveness, loss of confidential information can ruin the organisation's reputation, and if the organisation's systems are not accessible, that can lead to unprofitability. Data breaches often lead to revenue loss, jobs, lack of trust in essential digital processes, and even lost identity.

Consequently, a security breach is detrimental to the affected devices and the entire organisation (Banfield, 2016). According to Ifinedo (2015) and Safa et al. (2016), the failure of users to adhere to the company's information security policy and equivalent instructions unwittingly promotes cybercrime against their organisations. This exposes users to identity theft if personal information lands in the wrong hands. In addition, users who practice unsafe computing conduct in non-work settings invite hackers to their personal computers and the organisation's systems (Liu, Wang & Liang 2020). As a matter of fact, following uncompromising security guidelines comes at a price, but it will not compromise the organisation's revenue (Alghamdi et al., 2020). (Puhakainen & Siponen, 2015; Moody, Siponen & Pahnla, 2018). Generally, data breaches occur because users are negligent, ignorant, unaware, mischievous, apathetic and resistant (Safa et al., 2016). The biggest concern in information security is the poor security conduct of users. Organisations face reputational loss and financial loss due to data breaches. Organisations can even close their business due to cyber-attacks, losing a laptop with valuable and confidential information, or if a database containing sensitive information about clients is leaked online, which could have dire consequences on the organisation's future (Alghamdi et al., 2020). Security depends on every user to be successful. A single user whose behaviour is against security guidelines can compromise the entire security chain. That user's conduct can expose the security system and can be exploited by hackers (Balozian & Leidner, 2017). Users' ignorance is always at the centre of security breaches in many incidents. People play a pivotal role in information security

management. Employees' behaviour can affect the organisation positively or negatively (Safa et al., 2016). Employees who demonstrate poor security conduct may commit information theft with malicious intent and violate access policy, which is a serious threat to business organisations. However, if employees adhere to security policies, awareness, and training, that behaviour will positively impact information security (Soomro, Shah & Ahmed, 2016).

Furthermore, dissemination of improper, incorrect, or classified information, information system outages, a compromise in the integrity of information, significant economic loss and inability to deliver services are the repercussions of human errors in information management (Rupere & Muhonde, 2012; Abdelsadeq et al., 2019.). Blythe, Coventry and Little (2015); Votipka et al. (2018) further note that data leaks of secret information can be more harmful and distressful to organisations and individuals. In addition, companies keep information about their clients and business operations, e.g., intellectual property. Disclosing this classified information can have a negative impact on business operations and stature. If users fail to uphold cyber-security policies (CSP), the organisation's security valuables may be at risk (Charlette, 2015; Donalds & Barclay, 2022). In essence, the inappropriate use of data and information stored in an organisation's information system and associated technologies can have unwanted ramifications, such as bad publicity, loss of credibility, and legal and regulatory concerns (Ifinedo, 2015; Ifinedo et al., 2017).

1.9.4 Approaches that encourage compliance

Information security training and awareness of what is at stake in information security are key to users' compliance with information security policy (Merhi & Midha, 2012; Bauer & Bernroider, 2017). Soomro et al. (2016) believe that security training raises awareness and encourages proper security conduct and access policy contravention. Information security compliance ensures that various elements of information security are synchronized to achieve the optimum security goal and ensure IS processes are working (Alkalbani, Deng & Kam, 2014; Bhaharin et al., 2019). This way, compliance management is closely linked with the conduct of users that can either be adherent or disobedient to an organisation's security guidelines (Kim & Kim, 2020). Hence it is essential to enforce IS compliance. Figure 1.13 depicts an information security compliance framework known as the functional application of information security standards and policies for protecting information in organisations, a dynamic technique generally employed (Alkalbani, Deng & Zhang, 2016).

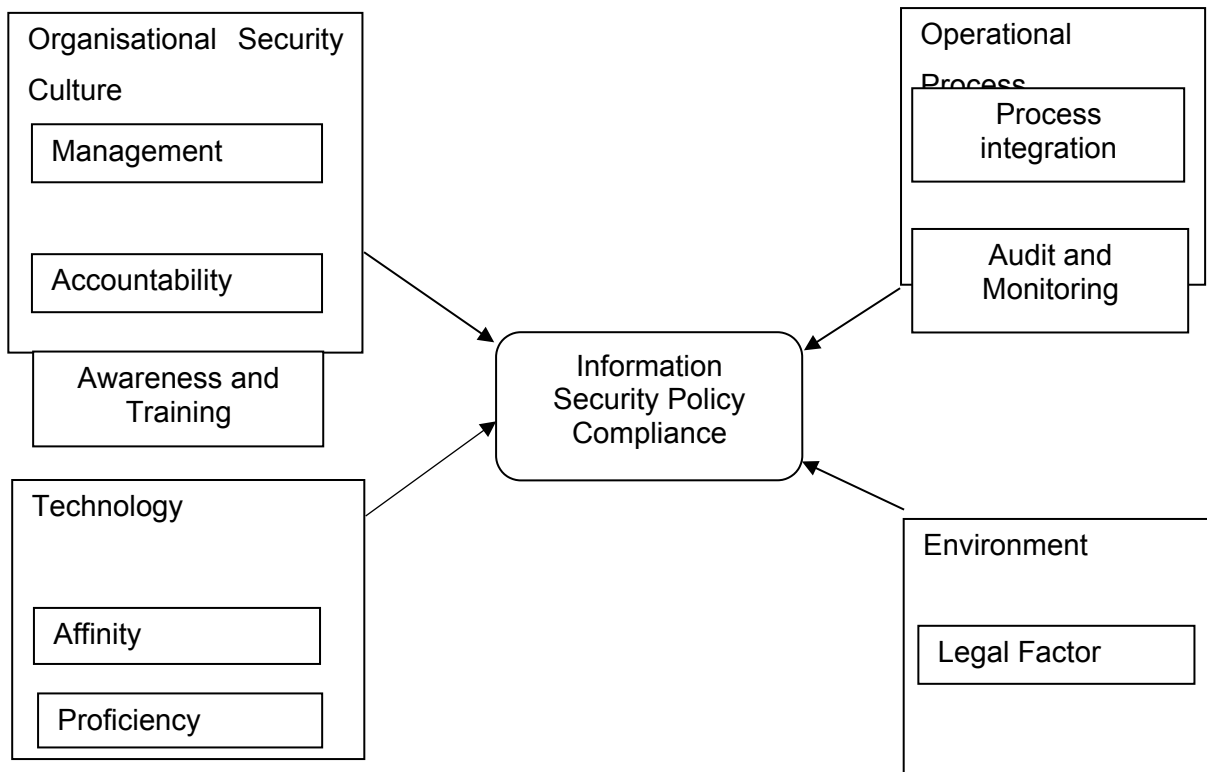


Figure 1.13: Information Security Compliance Framework adapted from (Alkalbani, Deng & Zhang, 2016)

A key aspect of information security research is to develop methods that will impel end-users, employees and consumers to protect better their individual and organisational information resources (Boss et al., 2015; Moody et al., 2018). Awareness solutions should ensure that employees are well-equipped to combat cybercrime and safeguard information valuables. Acquiring security expertise should be seen as enhancing an employee’s profile and competence development. Therefore, organisations have an obligation to ensure that employees can see the value of security expertise instead of seeing them as a daunting task that competes with their primary function (Pham et al., 2017). Compliance can only be achieved if users are encouraged to contribute and comply with information security rules, implementations, and controls. This will ensure that information security management is functional and efficient. Research has shown that users can only improve their security conduct if they are regularly exposed to effective awareness training and other awareness mechanisms and tools (Al-Omari et al., 2013; Blythe et al., 2015; Voptika et al., 2018).

Puhakainen and Siponen (2015); Alyami et al. (2020) posit that imposing disciplinary measures when security policies are violated should be necessitated. Therefore, security policies should be enforced throughout the organisation, and compliance with security policies should be part of the job requirements and performance review. To achieve this, compliance should not be seen as an IT function. Therefore, executive management needs to embrace information security. This essentially means ensuring that awareness levels of all employees are raised so that security compliance becomes a fundamental aspect of the organisation. In other words, security should be integrated with the organisational culture (Hamdan, 2013; Milov et al., 2019). For this to be possible, management must consider security as precedence. To achieve this, there are three crucial points that management and security professionals need to be aware of. Firstly, Information security should not be isolated from the organisation's culture. This means that security must be an essential part of the organisational culture (Tolah, Furnell & Papadaki, 2021). The best approach to achieving this is to pinpoint subparts of security policy that apply to every employee and can be enforced without interfering with employees' primary function. Accomplishing awareness and compliance requires training, incentivizing employees and total backing of a security policy by the entire management (Alkalbani, Deng & Kam, 2018). As soon as employees inherently adopt a security policy, management can gradually incorporate the rest of the policies until all procedures relevant to the day-to-day conduct of employees are adopted successfully (Tenzin, 2021). Secondly, for an organisation to successfully integrate security into its culture, top management needs to drive compliance and ensure that it filters down to the lower levels of the organisational structure (Tolah et al., 2021). With that said, it is important to get the buy-in of middle management, and chief information officers can assist drive the change. Thirdly, an organisation with an effective security policy will improve efficiency, and applications will become less expensive to maintain. Lastly, an effective security policy will help enhance the reputability of the organisation (Melnyk & Shmatkovska, 2016).

Complying with the security policy should be part of the annual review process for every employee and management. Furthermore, management must observe users' compliance, recognize compliance and penalize security misconduct. At first, adherence to the security policy should be recognized, but ultimately it should be a predicted norm. During the initial stages, non-compliance should be treated as an opportunity to address areas of uncertainty. However, if it persists, it should be punishable (Hwang et al., 2017). The methods that encourage compliance are the development philosophy and deterrence philosophy. The development philosophy is positive in its approach and focusing is on encouraging users to comply. Deterrence philosophy, on the other hand, is a more negative approach because it

creates fear in the event employees fails to comply. A typical example of development philosophy would be explaining the benefits of compliance, and deterrence philosophy would outline the penalty if employees fail to comply (Balozian & Leidner, 2017).

Alkalbani, Deng & Kam (2018) note that the three primary aspects that support the adoption of organisational security culture are: management commitment, accountability and information security awareness.

1. Management commitment could be evaluated by personnel's interpretation of endeavours that are taken by management to achieve information security compliance as reflected by management support, participation, goal alignment and efficiency.
2. Accountability can be evaluated by users' awareness of the level of completeness of the information security policy for providing necessary guidance in information security conduct, clarity and intelligibility of the roles and responsibilities, suitability of punishment for contravening ISP, and the enforcement of information security policies and procedures across the organisation.
3. The awareness of information compliance can be measured by how users view aspects of information security compliance training methods. Users' view of the efficacy of training methods indicates the effects of training programs that promote organisations' information security goals. In contrast, users' outlook on the effectiveness of the methods indicates the successful presentation and structure of the training methods.

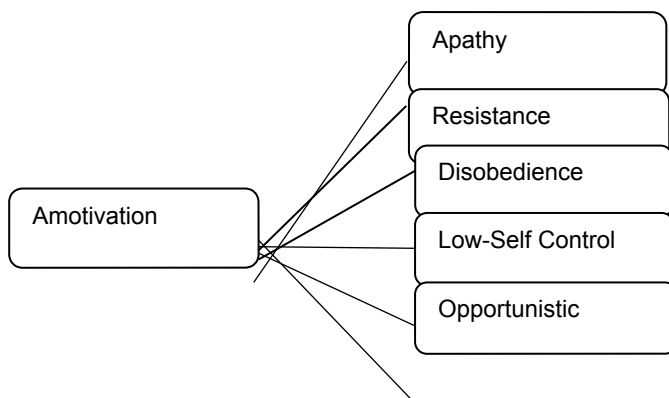
Organisational aspects, like the development of security policy, awareness, compliance, and implementation of best practices, basically form a benchmark for information security. An organisation is responsible for these activities; therefore, it is recommended that when adopting information security management, it should consider all the elements holistically (Soomro et al., 2016). Moreover, Kretzer and Maedche (2015); Whitman and Mattord (2021) detail six classifications of security measures: training, informational materials, controls, security agents, sanctions and incentives. Training, one area that has been researched extensively for ensuring user compliance with information security policy, has to be training. This approach usually includes educational activities to advance users' compliance with ISP. Informational Materials refer to practical examples of acceptable compliance conduct and typical misconduct.

Examples include posters, leaflets, gadgets, and intangible assets like emails to disseminate information regarding ISP and security compliance conduct. Controls regularly monitor compliance conduct and carrying out regular controls can help assess the compliance conduct of users. Companies have realized that to keep up with the perpetual threat of cybercrime, they need a concerted effort that combines technical, administrative and physical controls. The nature of the threat decides whether the organisation should defer some controls to external parties or maybe internal employees can carry out certain controls. Security Agents and security staff are responsible for propagating information about information security policies throughout the entire organisation. They are knowledgeable about security matters, their fellow workers' tasks, and work routines. The role of security agents may differ from organisation to organisation, but their core duties include training and supporting colleagues and encouraging them to comply with ISPs. Sometimes, they may assign users rights and permissions depending on operational requirements. Sanctions and deterrence-based techniques believe that fear of punishment dictates if users will comply with ISP. Based on avoidance motivation philosophers, users are naturally inspired to steer clear of threats. Rewards studies have established that rewarding security behaviour can improve compliance. Staff believes sanctions are punishment for non-compliance, whereas rewards are generally seen as advantages for compliance. Padayachee (2012); Hengstler, Nickerson and Trang (2022) describe the key areas of security behaviour as amotivation, extrinsic and intrinsic motivation.

Amotivation is the inability to carry out a specific task because the task is ineffective or due to incompetence.

Extrinsic motivation implies that employees carry out tasks because it yields a distinguishable end result.

Intrinsic motivation implies that users carry out a task because it is naturally fascinating and exciting. Figure 1.14 below provides a classification of security-compliant behaviour.



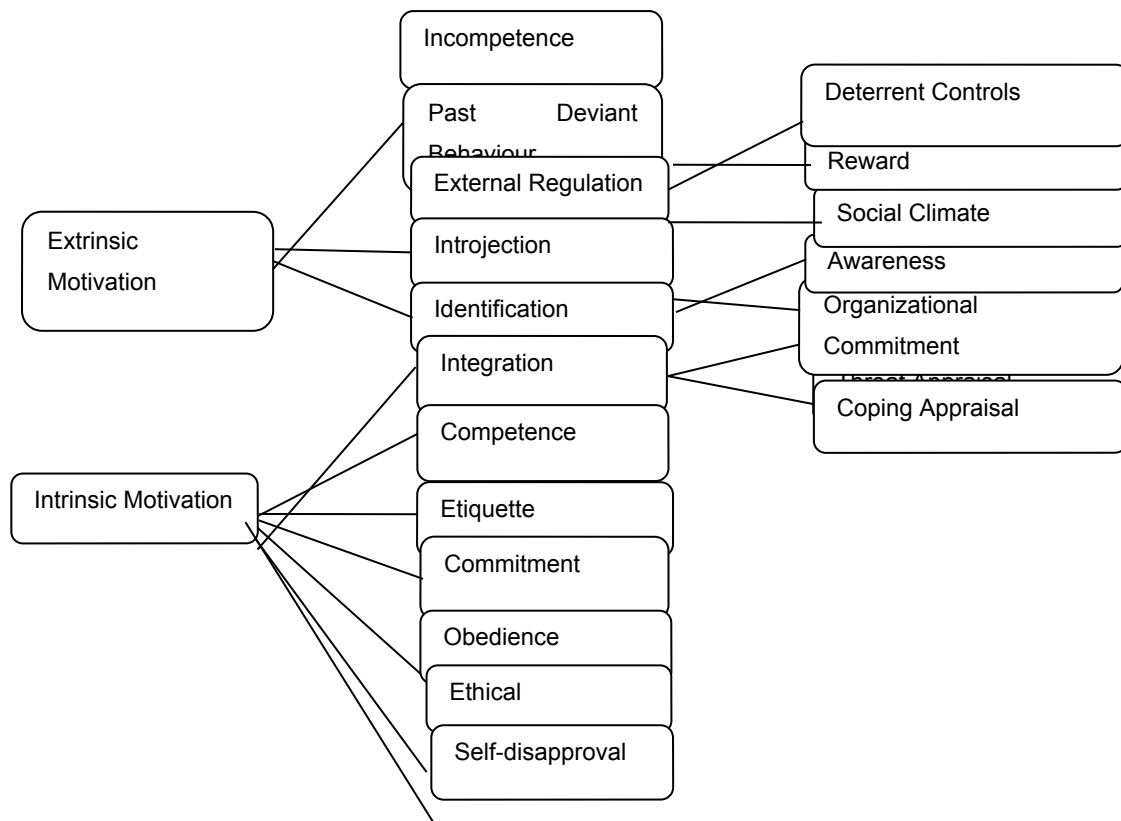


Figure 1.14: The Classification of Security Compliant Behaviour adapted from (Padayachee, 2012)

1.9.5 Acceptable user security behaviour

Ruighaver, Maynard and Warren (2012); Safa et al. (2016) argue that ISPs, especially acceptable use policies (AUP), are designed with too much emphasis on deterrence. Still, in the application, they have shown over-reliance on deontological ethics. That is, users will take the correct action. Moreover, Merhi and Midha (2012); Gangire, Veiga and Herselman (2020) add that if users are familiar with the regulations, they feel compelled to abide by them. Hence, it is vital to have comprehensible and unambiguous security policies (Abraham & Nair, 2014; Alotaibi, 2019). Acceptable information security behaviour should preferably be fused with other technology features (Safa et al., 2016). To practice acceptable user behaviour, users must have the necessary skill and expertise (Abraham & Nair, 2014; Rajasooriya, Tsokos & Kaluarachchi, 2017). Nasir and Fahmy (2021) postulate that insufficient information concerning ISP means employees cannot perform their primary function securely. Banfield (2016) advises that employees must know what is expected of them in the fight against cybercrime and how to deal with any possible threat.

Conscious care behaviour is a successful method that is used to thwart cybercrime. Conscious care encourages users to be aware of the repercussions of their security behaviour and to exercise vigilance when using the system or the internet. Information security awareness expertise and understanding are key in this realm (Safa et al., 2016). In addition, Ruighaver et al. (2012); Maynard et al. (2018) highlight the importance of sound judgment that employees are required to apply. Also, employees are expected to be accountable for any form of deviation from the set security rules. Employees should also be sensitized about the necessary steps they can take if they pick up any behaviour deviant from the norm or see a need to impart knowledge to their colleagues. Alfawaz, Nelson and Mohannak (2010); Gangire, Veiga and Herselman (2020) point out four methods to group individual security: Not knowing-not-doing method, Not-knowing doing method, Knowing-not doing method and Knowing-doing method.

Not knowing-not doing: in this mode, the user does not have the necessary knowledge with regards to the ISP of the institution and is unaware of security requisites. Hence the user is bound to commit security mistakes and improper security conduct (Gangire et al., 2020).

Not knowing-doing: in this mode, the user has no knowledge of ISP and has not been exposed to the organisation's information security requisites. However, the user maintains proper conduct by abiding by the regulations (Ahmad et al., 2016).

Knowing-not doing: Here, the user has the fundamental knowledge of ISP, the security expertise needed and is aware of the organisational security requirements. The user maintains improper security conduct or contravenes the ISP (Gangire, Veiga & Herselman, 2021).

Knowing-doing: here, the ISP is established and is fully distributed to the user. Hence, the user can maintain proper conduct. Thus, the user abides by the set security guidelines and has no plans to breach the ISP regulations (Alotaibi, 2019).

1.9.6 How to improve users' security behaviour

Encouraging the attitude of compliant behaviour with ISP is not something that can be easily achieved. Risks and threats always vary; information security awareness is not a static activity, so awareness material must be kept up to date. Awareness processes should be integrated with the organisation's culture to keep clients updated. Nasir and Fahmy (2021) assert that users' conduct must be controlled and supervised to ensure it is compliant and in line with ISP requisites. There are two approaches to improving users' conduct and tackling security

violations: information security awareness and/or computer security awareness. Employee awareness of security policies, security education, training, and awareness (SETA) process are crucial to improving security compliance (Charlette, 2015; Angst et al., 2017). Ifinedo (2015); Furnell et al. (2018) state that in organisations where top management shows the backing of ISP, the security conduct of the users improves significantly. Similarly, Alotaibi (2019) advises that management should drive the ISP and have a clear direction pertaining to specific areas that can significantly affect the institution, including users, the organisation's culture, security policy and procedures and the technical environment. According to Charlette (2015); McSweeney (2018), top management's belief in ISP activities motivates and encourages users to comply and improve their conduct. Figure 1.15 illustrates the relationship between awareness, training, and compliance. Also, management support improves compliance behaviour.

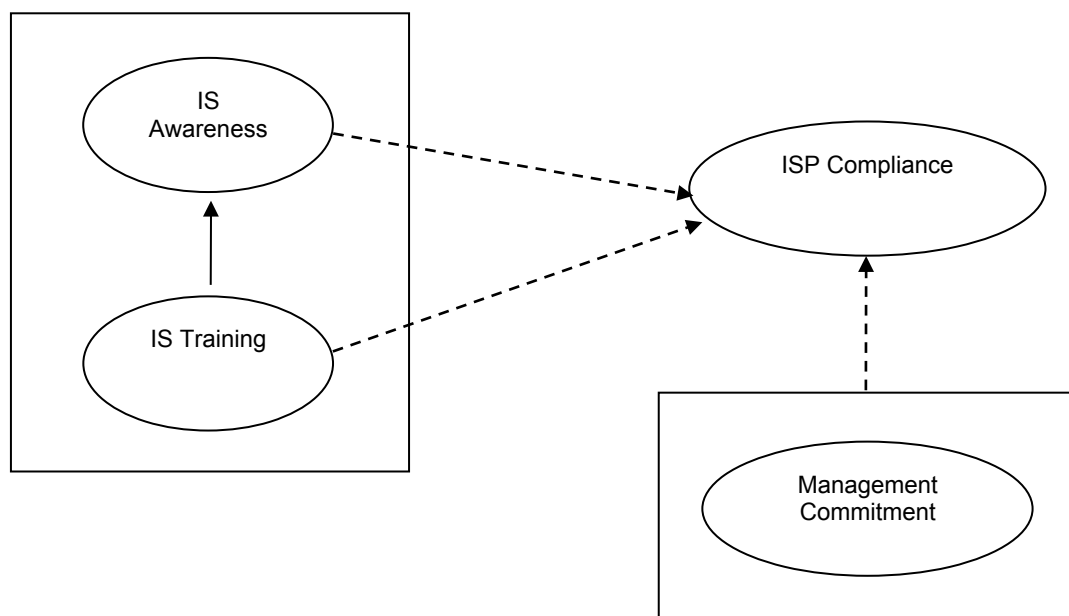


Figure 1.15: Compliance behaviour adapted from (Charlette, 2015)

Improving employee awareness and equipping them with data protection techniques in the technical and human realms is a proven risk-mitigation approach. It also reduces cost and the time needed to plan for every possible contingency (Banfield, 2016). Table 1.4 depicts a broad organisational defence tactic that preceded end-user behavioural security measures (Banfield, 2016).

Table 1.4: Information Security Awareness adapted from (Banfield, 2016)

Information Security Awareness	Operational Measurement
Organisational IS equipment installed: technical controls used to manage security incidents	Employees understanding of the role performed by technical controls (Intrusion Prevention Systems, Intrusion Detection Systems, Firewalls)
Organisational IS posture: security culture of the organisation.	Employees' awareness of Information Security Policies
Organisational IS expertise: non-technical controls that rely on users' level of awareness	Employees' expert knowledge of non-technical security tools and techniques
Security Self-efficacy: user's ability to abide by	Employees' security and risk awareness

IS rules	
Policy, Governance and Compliance: non-technical guidelines that the organisation adopts to ensure users can protect resources.	Employees' understanding of ISP and regulations
Benign damaging security conduct: non-malicious intent that poses a threat to the organisation	Employees understanding of security threats (social engineering, data privacy, encryption, malware programs)

1.10 Research Methodology, Strategy & Design

1.10.1 Research Methodology

This research study will adopt a positivist approach. The approach is followed by positivist research concerned with control and predictability (Blaxter, Hughes & Tight, 2012). The Oates model shown in figure 1.16 will guide the research project. The figure shows how the model will be adopted for this research study. The Oates model supports the positivism paradigm. It caters for the researcher's experiences and motivations. Review of pertinent literature. It allows the formulation of the hypothesis and testing the hypothesis to explain the observed phenomenon using quantitative data analysis methods.

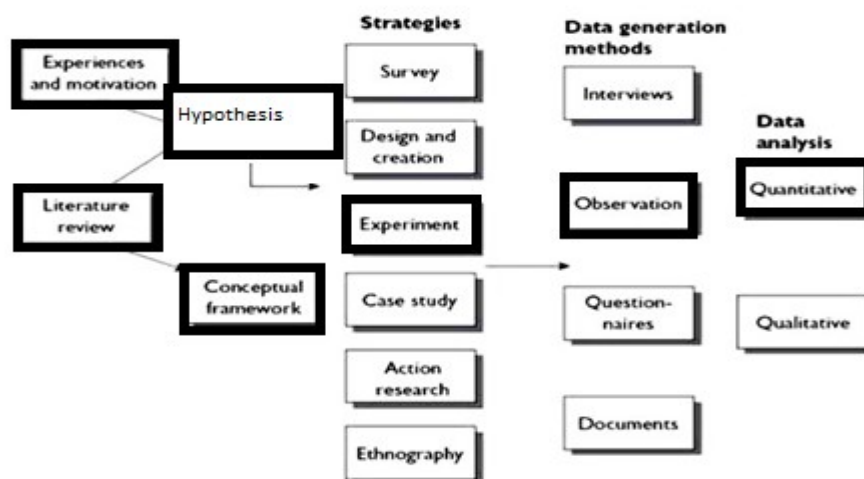


Figure 1.16: A pictorial representation of the methodological process (Oates, 2006)

1.10.2 Research Strategy

The research strategy of this study is quantitative. It involves the formulation and testing of the hypothesis. The research strategy is grounded in the methodological process of the Oates model discussed in figure 1.17. The Oates model informs the paradigmatic direction a researcher undertakes to complete a research project successfully. The Oates process model is designed explicitly for Information Systems or computer research projects (Oates, 2006). Figure 1.9 explains the research strategy of this research study. The strategy is to review pertinent literature, formulate a hypothesis, test the hypothesis, and based on the outcomes, accept, or reject the hypothesis.

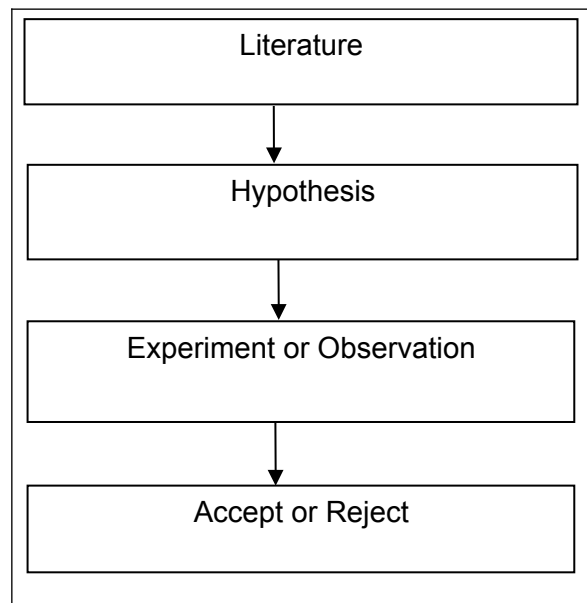


Figure 1.17: Research Strategy

1.10.3 Research Design

The study will adopt a two-group experimental research design. The participants will be drawn from government entities in Cape Town. This will be a two-group design where the participants will be randomly selected to form two groups, i.e., the control and experimental groups. The two groups will receive similar information security training about password policy, BYOD policy and phishing. BYOD enables employees to use personal devices to access and share organisational resources (Siddiqui, 2015). Phishing is a social engineering attack that exploits human vulnerabilities to steal confidential information or install malicious programs (Khonji & Iraqi, 2013). One group of users, the *control group*, will only receive information security training. The other group of users, the *experimental group*, will also receive information security training; however, the experimental group will further be exposed to a chatbot (treatment) to

test the hypothesis. The units of analysis will be the individual end-users of the respective government entities. The independent variables for this research study are strong passwords, attachments and scan devices. The dependent variables are compliance and non-compliance. The study will use MS Excel and a chatbot to conduct the experiment.

1.11 Data Collection

The method for data collection will be based on the principles of experimental study, and therefore, the observation method will be used to collect primary data. Qualitative data will be collected as part of quantitative research. Qualitative information gathered about password policy, BYOD policy, and phishing will be quantified. The study is intended to measure compliance against users' non-compliance. Based on the user's level of awareness, compliance, and a general understanding of information security policy, appropriate action will be taken. The study will employ a non-participant observation approach to collect data, according to Kumar (2011), when a researcher does not actively participate in group tasks. Still, instead, the researcher passively observes the proceedings. Wilkinson and Birmingham (2003) add that the observation method involves a lengthy process in which participants' behaviour is closely monitored, and data is gathered according to a specific method. Shull, Singer and Sjøberg (2008) point out that the advantages of the observation method are:

1. Implementation is less complicated

Spross (2014) notes that the observational approach is simple and easy to apply.

2. Provides swift results

Observation is precise and, thus, only requires that a researcher judge the behaviour's occurrence (Muhammad, 2016).

3. It does not need any special apparatus

The observational method does not require any special equipment to record data (Shull, Singer & Sjøberg, 2008).

The reason for selecting the observational approach is because the nature of the study and the problem the research is trying to address are more apt for the observational method.

1.12 Data Analysis

A quantitative analysis approach will be used to analyse the data. Blaxter, Hughes and Tight (2012) define quantitative analysis as a technique that necessitates using statistical methods to analyse data. The data will be collected through the observation method and will be analysed using quantitative methods. Data will be collected on the following variables strong passwords, attachments, and scan devices. Microsoft Excel data analysis will be used to analyse the gathered data. The captured data will be analysed based on the following:

1. User compliance
2. User non-compliance

Statistical analysis methods will be used to interpret the data of the two groups. Inferential statistics will be used to test the hypothesis, specifically a t-test. The t-test is employed when testing the mean difference between two groups (Marczyk et al., 2005). T-tests help researchers determine if there is any statistical difference between the means of the two groups. The t-test can conduct non-directional or two-tailed tests (Bhattacharjee 2012). Welman et al. (2005) added that the t-test helps researchers ascertain whether the mean difference between the two groups is due to the intervention or simply by accident.

1.13 Ethical Consideration

Kumar (2011) explains that ethics or ethical conduct suggests abiding by acceptable principles of a particular profession or society. In research, ethical considerations play a significant role during the recruitment of participants, when administering the treatment, and when delivering the study results (Welman et al., 2005). The study will involve data collection; therefore, ethical consent will be solicited from all concerned quarters, such as the Cape Peninsula University of Technology and the entities from which the participants will be drawn. A letter detailing the purpose of the study, the criteria used to identify entities, and the importance of partaking in the study will be sent to respective government entities. The letter will request seeking permission to conduct research. The letter will briefly explain the aims of the study and what is expected from the participants granted the request to conduct research is accepted. The research participants can choose to participate in the study or not and withdraw at any time they feel to

do so. Also, the aim of the research will be fully explained to them, and their confidentiality will be guaranteed. Using the chatbot will by no means violate the users' privacy; thus, a chatbot will not track users' activities on the system. In addition, the study will not expose the participants to any risk or harm.

1.14 Outcomes, Contribution, Significance

1.14.1 Outcomes

The desired outcome of the study is to improve user compliance behaviour through a chatbot. If users receive a constant reminder about ISP, compliance will not be seen as a periodic task that needs to be performed once or twice a year. Therefore, another study outcome is ensuring users receive regular ISP updates.

1.14.2 Contribution

The study will contribute to the ongoing struggle to improve compliance among IT users and thus contribute to future research around cybersecurity. The study will also benefit the government entities that participated in the research study.

1.14.3 Significance

The study is expected to raise Information Security Awareness and improve Information Security Policy Compliance. This research is expected to equip users better to deal with phishing and adhere to password and BYOD policies.

1.15 Summary

This chapter introduced the background to the study, the role of chatbots in security, the problem statement, aim, objectives, hypothesis, current literature, research methods, ethics, data collection and analysis.

1.16 Thesis overview

This thesis is arranged in the following manner: chapter one covers the introduction and background to the research problem. The research aims and objectives are outlined. Chapter two discusses the current literature and its impact on recognizing compliance and punishing non-compliance. The chapter looks at the use of chatbots in education and training. Chapter two also discusses a systematic literature review to address questions pertinent to the study. The review protocol, which outlines the methods employed in the review, is discussed. Inclusion and exclusion criteria are explained to justify study selection. Chapter three provides a roadmap for all the methods the study adopted to fulfil the requirements of this research project. Chapter four discusses the process that was undertaken to conduct the research experiment. Chapter five provides a detailed report of the results of the investigation. Chapter six analyses the results of the experiment and discusses the implications of the results.

CHAPTER TWO LITERATURE REVIEW

2.1 Introduction

This chapter aims to provide an overview of the field and identify the research gap. A traditional review obtained the field overview and identified the gap through a structured literature review.

2.2 Overview of the field

The purpose of the literature review is essential to allow a researcher to consider what has been done in an area, what can be gained from the literature and how one could situate their study in the context of other research studies. Similarly, this literature review explores issues surrounding information security awareness (ISA) to determine feasible ways to improve information security policy compliance. In recent years organisations have paid serious attention to enforcing information security compliance (Hengstler & Pryazhnykova, 2021). Kuppusamy et al. (2020) note that this means applying information security standards, procedures and policies to safeguard organisational information resources adequately. Over time, security researchers and practitioners have tried to understand why employees' compliance behaviour is not in line with organisational security policies and mechanisms (Crossland & Ertan, 2018). There is a growing consensus that the weakest link in protecting organisational information resources is the individual user (Warkentin et al., 2016). Eliana (2020) believes that employees' poor compliance behaviour poses a serious risk to organisations' efforts to protect systems and data.

The advent of chatbots has created a new dimension to artificial intelligence (AI) research. Chatbots are intelligent interfaces that can coherently communicate (Behera,2016). Chatbots have many advantages, namely, one-to-one communication, 24 hours a day, seven days a week, user interests, responses and profiles, customized offers that can be targeted directly and personally to users, time zones, opening times and waiting for loops of call and service centres and supporting and training purposes for employees (Zumstein & Hundertmark, 2018b).

This chapter seeks to review the extant literature in the area of ISA. It is structured as follows: the impact of recognizing compliance and punishing non-compliance, chatbot, types of chatbots, uses of chatbots, chatbot framework, the chatbot in education and training or guidance and chatbot implementation.

2.3 The impact of recognizing compliance and punishing non-compliance

To improve user compliance behaviour, organisations have devised creative innovations that intend to motivate users to maintain a sound security posture. These activities include awareness programs and other motivational methods (Ogunnoiki, 2019). However, these programs have failed to yield the desired outcomes, and consequently, users' compliance levels have not improved. (Goel et al., 2020). Balozian and Leidner (2017) argue that information security relies on two approaches to enforce compliance: deterrence and development. Deterrence creates fear among users because it states that any security violation will be penalized. At the same time, the development approach encourages employees to remain compliant by recognizing compliant behaviour. Recent studies have shown that rewards have an insignificant impact on security compliance (Goel et al., 2020). Pham et al. (2017) propound that using fear to encourage compliance only has a short-term effect and does not address the issue of ongoing compliance. Topa and Karyda (2016) conclude that pertinent literature has failed to provide decisive findings on the effectiveness of rewards on user security conduct.

2.4 Chatbot

A chatbot or chatterbot is a software application that intends to give a user the impression that they are interacting with another human being. Chatbots are either text or voice-based (Kowalski, Pavlovska & Goldstein, 2013). According to Doshi et al. (2017), the three major components of a chatbot are the user interface, an interpreter and a knowledge base. The main objective of a chatbot is to simulate human conversations and keep users engaged (Ignatov et al., 2014). In addition, Lyons (2017) also states that a chatbot's key features are ease of use, timely response and user-friendliness. Chatbot conversations with users should flow, be uncomplicated and ensure quicker response time to ensure that users do not get bored. Above all, bots should provide answers to users' queries without complications or misinterpretation

from the chatbot. Chatbots are classified through various parameters such as the knowledge domain, service provided, goals, and responses. The knowledge domain is based on Chatbot's knowledge (Okonkwo & Ade-Ibijola, 2021). There are two types of domains, namely the open and closed domains. The open-domain Chatbots deal with general topics and respond aptly to general queries. The bots in the closed domain are more concerned with specific knowledge domains and may be unable to address other domains. The service-based Chatbots are grouped into those that offer interpersonal, intrapersonal and inter-agent services. The goal-based Chatbots are further classified under informative, conversational and task-based Chatbots. The last category includes the Chatbots based on the input method and the responses generated (Sandu & Gide, 2019). Chatbots are created using artificial intelligence (AI), which is the algorithm behind their ability to mimic a human conversation (Meyer von Wolff et al., 2019).

2.4.1 Types of chatbots

Chatbots have two major designs, the first is simply a collection of rules, and the second is more modern and uses artificial intelligence (AI) (Sharma, Goyal, & Malik, 2017). The chatbot design based on rules is often referred to as a rule-based design, and the more advanced design is referred to as a self-learning chatbot. The rule-based model uses the if-else approach, while the self-learning model utilizes machine learning (ML) methods, which allow it to continue learning about whatever it runs into regardless of whether it is stored in the database or not (Thies et al., 2017). According to Babar, Lapouchnian and Yu (2011); Tangkittipon et al. (2020), bots can be categorised based on their sophistication and the intricacy required to formulate a reply to a query. Kottorp and Jaderberg (2017) highlight retrieval-based and generative-based as the two major designs of chatbots. A retrieval-based chatbot relies on the predetermined collection of replies and uses heuristics to select the most appropriate reply from a specified input. On the other hand, a generative model does not rely on predetermined replies to formulate a reply. Instead, it generates an appropriate reply based on the query.

1. Retrieval-based chatbots have a less complicated approach to their design and are often utilised in cases where a mere reply or steps to a query are needed.
2. Generative chatbots are somewhat convoluted in their design approach and often utilised in cases where a formulation of a peculiar and contextually suitable reply to a user query is needed (Ciayandi, Mawardi & Hendryli, 2020).

Kousa (2019) notes that machine learning (ML) can be classified into supervised, unsupervised and deep learning (DL). These are technologies that are used by chatbots. In supervised learning, bots receive natural language training and assistance by pre-labelling data. On the other hand, in unsupervised learning, bots do not need pre-assistance. Rather the application can be provided with any data, and it can classify it using algorithms like clustering, where objects that share the same traits are grouped, and a bot can create its own rules based on similarities and patterns.

2.4.2 Uses of chatbots

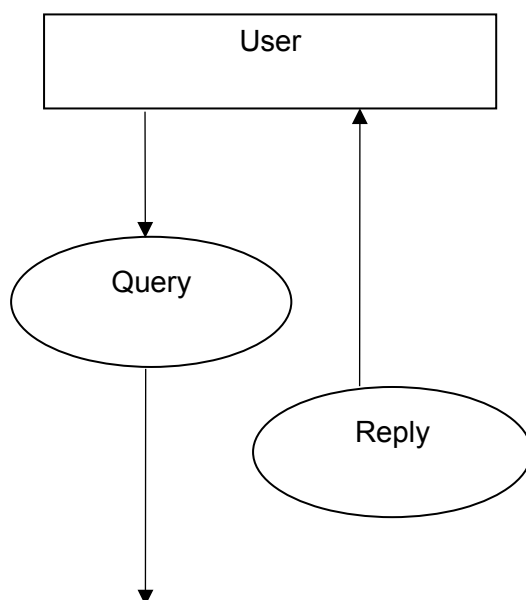
Many organisations have incorporated chatbots into their business strategy and rely heavily on using chatbots to dispense information about services and products and allow clients to start a purchase (Fiore, Baldauf & Thiel, 2019). Furthermore, Cunningham-Nelson et al. (2019) argue that FAQ chatbot is the most prevalent type. Many companies use FAQ chatbots to aid interaction between clients and the business entity so that clients can gain insight into the entity. Lyons (2019) suggests that contemporary chatbots are quite advanced and use natural language processing that can glean from user input. With APIs, chatbots can draw information about news, weather, and time. Some chatbots can complete orders and make reservations wholly using a chatbot interface. Several chatbots have been developed to assist with online learning, client service site, guidance and entertainment (Doshi et al., 2017). Moreover, there are also many positive purposes for which chatbots have been developed and used. They are used for offline troubleshooting, automated customer service and educational/pedagogical purposes (Malvisi, 2014; Brandtzaeg & Følstad, 2017). Sharma, Goyal and Malik (2017) add that chatbots can perform mundane tasks like calculations, reminders, and alarms.

Chatbots have been developed for many domains, like e-commerce, entertainment, and travelling. (Thies et al., 2017). Sannikova (2018) notes that chatbots are often incorporated into interactive systems of, for instance, virtual assistants, enabling them to naturally communicate or engage in casual conversations unrelated to the scopes of their primary expert systems. Kottorp and Jaderberg (2017) added that if a chatbot is deployed successfully, it can help automate specific functions such as education, information retrieval, business, e-commerce and amusement. Cohen et al. (2017) suggest that using chatbots to simulate a conversation could have a positive effect in the end because, in some cases, students find it challenging to share their online experiences. Han (2020) posits that AI-powered chatbots embodied with interactive

features, such as providing response feedback and probing responses, have been proposed to conduct conversational interviews and proved effective in elicitation.

The world of entertainment, commerce, the public sector, and educational institutions have promptly embraced the use of chatbots. Chatbots have shown the ability to partake in artificial intelligence contests (Rubesch, 2013; Brandtzaeg & Følstad, 2017). The proliferation of e-commerce has seen the widespread use of chatbots as virtual agents. The public sector has experimented with using chatbots as institutional information agents. These are more advanced chatbots that are deployed in expos, museums, and libraries. Moreover, these chatbots have been successfully deployed as virtual tour guides, virtual teaching assistants, and student services agents for distance learners (Moraes & Márcia, 2019).

Chatbots and AI have shown significant progress in areas that require artificial intelligence to accomplish functions ranging from making admission decisions to creating admission letters. This accelerates and automatizes tasks that usually require human resources (Robinson, 2019). Additionally, according to (Cahn, 2017), contemporary chatbots can act as *dialogic agents*, i.e. they should know and comprehend what the user wants. Chatbots are equipped with textual and oral inputs, which are translated using natural language processing tools to formulate suitable replies. *Rational agents* rely on an external base of knowledge and understanding (e.g., via corpora of data) to have competence in responding to users' queries. *Embodied agents* provide the function of existence and are of high importance in the case of ordinary users. Hence chatbots were initially given names like (ELIZA, ALICE, and CHARLIE). Modern chatbots are developed with more focus on language tricks to generate personas for chatbots, form trust with users, and create the feeling of an embodied agent (Andre & Pelachaud, 2016). Figure 2.1 shows a basic chatbot design.



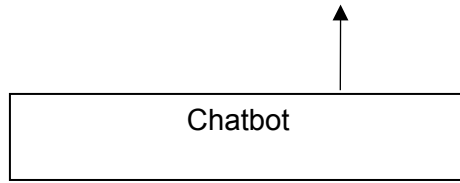


Figure 2.1: Use Case Diagram of Chatbot Design adapted from (Dahiya, 2017)

2.4.3 Key elements of a chatbot

Social, psychological, and behavioural impact factors and findings on communication between users and chatbots are discussed below. Team member, a bot that is seen as part of the team is more trustworthy than a bot that is merely seen as a technological application. If chatbots present more human-like conduct, users find it easy to trust the credibility of the information (Zumstein and Hundertmark, 2018b). Scope of the messages, users envisage a degree of politeness from a chatbot. Thus, users' expectations of a chatbot are that it should not provide too much information or bulleted responses. Still, it should provide accurate answers that correspond with the user's query in a courteous fashion. This requires a chatbot to understand users' preferences based on previous interactions and inquiries (Yen & Chiang, 2021).

Personality trait, a chatbot should be able to adjust its language to suit the different personalities of users. This means a chatbot should discern a user's personality throughout the interaction by using special codes and readjusting its personality to match the user's preferred terminology. The other option is for the chatbot to introduce a user to various personality traits, and a user can select the most suitable chatbot personality (Adam, Wessel & Benlian, 2021).

Specialists vs generalists, research has shown that users find a specialist answer to be quite plausible than a nonexpert's answer. Therefore, it is advised that chatbots should cater to various topics and be able to interact at an expert level. Thus, the natural language output of chatbots should be generated professionally and expertly with human characteristics (Zumstein and Hundertmark, 2018b).

Gender stereotypes: it is expected that future chatbots will be able to discern users' expectations based on gender traits in human-computer interactions (HCI) (Yen & Chiang, 2021).

Credibility, users judge the credibility of a chatbot by its ability to provide adequate answers and ask different questions. Users will lose trust in the chatbot and discontinue using it if a chatbot fails to address and find solutions to users' queries and challenges. Users' expectations of a chatbot are that it should be able to learn from past interactions and should not always repeat questions. The trustworthiness of a chatbot depends on its ability to accurately construe users' questions and requests and come up with helpful and informative replies (Fiore et al., 2019).

Emotions, bots earn more credibility when they can show a bit of emotion. Chatbots should be able to adjust to a user's mood. Therefore, chatbots should display joy, gentleness and happiness to improve engagement and the relationship between the user and a chatbot. Additionally, a bot should be able to show sympathy and change its behaviour according to situational demands and caring. AI-powered bots use machine learning features for sentiment detection, which helps them detect a user's state of emotion and respond almost as efficiently as a human operator (Følstad, Nordheim & Bjørkli, 2018). Paikari and Van Der Hoek (2018) identify three types of chatbots:

Information, information chatbots help developers discover information that can be pertinent to accomplishing the task.

Collaboration, collaboration chatbots enable developers to collaborate and interact effectively.

Automation, automation chatbots assist developers in managing tasks that impact some type of change in one or more artefacts they are working on. In addition, Fiore et al. (2019) point out the transparency of a chatbot as the most important requisite for a chatbot to gain trust and be accepted by users.

1. A chatbot has to make a user aware that it is communicating with a robot.
2. A chatbot needs to proactively state its capabilities so that users know what to expect.
3. A chatbot should include a *proactive* conversation approach, i.e., the chatbot should take charge of the conversation and guide and support the users.
4. A chatbot should communicate in a language that is appropriate for its audience and meet the requirements of the users and corresponding use cases.

2.5 Chatbot Framework

Chatbots are developed using Artificial Intelligence Markup Language (AIML) and Latent Semantic Analysis (LSA). AIML and LSA-designed chatbots are mostly basic in their design and often deal with common inquiries like how are you? How can I help you etc.? This type of design is also suitable for cases where a chatbot provides random answers for the same query. LSA is used to find similarities between words as a vector representation (Ranoliya, Raghuwanshi & Singh, 2017). Vector representation enables words to be displayed in continuous volumes (Garten et al., 2015). Similarly, AIML is developed based on the concept of extensible markup language (XML), which is utilized to create conversational agents artificially. AIML-designed chatbots are more popular due to their light-weighted design and less costly configurations. AIML has a group of data objects referred to as AIML objects that outlines computer programs' conduct (Doshi et al., 2017). AIML's main design approach is based on minimalism, and thus AIML is arguably the most elementary bot language (Sharma et al., 2017).

One of the most widely used frameworks which fuse these perspectives is the PARAdigm for Dialogue System Evaluation (PARADISE). First and foremost, PARADISE estimates subjective factors such as (i) ease of usage, (ii) clarity, (iii) naturalness, (iv) friendliness, (v) robustness regarding misunderstandings and (vi) willingness to use the system again. It does so by collecting user ratings through the distribution of questionnaires (Shah & Shah, 2019). Second, PARADISE seeks to objectively measure bot efficacy by increasing task success and reducing dialogue costs (Cahn, 2017). Lommatzsch (2018) points out that frameworks such as Amazon Lex ("Alexa") 2 and Google DialogFlow3 design cater to a limited number of questions. Users can teach their personal chatbots to learn their wording and adapt to their preferred features. Typically, these frameworks are mostly suited for narrow domains characterized. Hence a significant number of training examples for all user objectives should be supplied. Microsoft Bot Framework enables chatbots to be developed and installed using Microsoft Azure. Once the chatbots are hosted on Azure, it becomes much easier to host them on different platforms like Facebook Messenger, Skype, Slack, and more (Lyons, 2017).

Chatbot frameworks are software frameworks that define a predetermined collection of tasks that reduce the intricacy of developing a chatbot, such as the NLP engine (Doshi et al., 2017).

Q n A Maker – a cloud-based framework designed by Microsoft that enables a mere Q&A chatbot to be developed through FAQs, URLs and structured documents (Shah & Shah, 2019).

Dialogflow – a well-known cloud-based framework designed by Google that is purely to utilize and enables incorporation with various platforms (Thorat & Jadhav, 2020).

Rasa NLU & Core – an open-source framework designed for the python development environment. It is a high-powered toolkit with a steep learning curve (Cahn, 2017).

Wit.ai – a cloud-based framework designed by Facebook that has similarities with Dialogflow but has limited features compared to Dialogflow. It performs well when paired with Facebook Messenger (Lyons, 2017).

Luis.ai - a cloud-based framework designed by Microsoft, its functionalities are comparable to Dialogflow and Wit.ai (Thorat & Jadhav, 2020).

Botkit.ai – Like Rasa, Botkit.ai is a programming library using Javascript. However, Botkit.ai comes with a graphical user interface (GUI) (Cunningham-Nelson et al., 2019). Table 2.1 draws a comparison of popular chatbot frameworks.

Table 2.1: Comparison of common chatbot frameworks adapted from (Cunningham-Nelson et al., 2019)

Name	Organisation	Licence	Ease of Use	OTB Integration	Open Source	Popularity	Web Based	Language
OnA Marker	Microsoft	Free	High	Yes	No	Moderate	Yes	C#
Dialogflow	Google	Free	High	Yes	No	High	Yes	JavaScript
Rasa	RASA	Free	Low	No	Yes	High	Yes	Python
Wit.ai	Facebook	Free	High	Yes (Facebook)	No	High	Yes	JavaScript
Luis.ai	Microsoft	Free	High	Yes	No	Moderate	Yes	JavaScript

			h			e		pt
Botkit.ai	Botkit	Free	Low	Yes	No	Moderate	No	JavaScript

2.6 Chatbots in education and training

Cunningham-Nelson et al. (2019) argue that the utilization of chatbots to improve learner interaction has recently seen a rapid rise, especially in today's world, where tech-savvy learners depend entirely on social media and instant messaging. Additionally, Ignatov et al. (2014); Mai (2022) observed an improvement in users' attitudes, particularly when chatbots are utilized in an e-learning environment about security conduct. Kowalski et al. (2013); Lorenzo and Gallon (2019) postulate that chatbots can provide extra features to supplement computer-based and online awareness training. Ignatov et al. (2014); Mai (2022) found that chatbots could provide security awareness and training. According to Winkler and Söllner (2018), chatbots should cover context information to improve cognitive and affective learning outcomes. Therefore, this suggests that a chatbot needs to consider learners' cognitive and emotional status to ensure they achieve their learning objectives.

In educational environments, studies have proved that purpose-built chatbots can be deployed in various learning areas and educate students in different fields (Rubesch, 2013, Lorenzo & Gallon, 2019). Chatbots can be grouped into those with education intentionality and those without. Chatbots without education intentionality are designed to serve administrative roles like guiding and assisting students. Chatbots with education intentionality serve to promote teaching and learning (Sandu & Gide, 2019). Chatbot interactions can help identify everyday user challenges and improve course material for human workers (Lyons, 2017). Certain chatbots can monitor user input on instant message (IM) channels and react to specific commands or patterns. Some chatbots can contribute to an IM channel based on external events that appraise the users. Additionally, chatbots can assist in performance monitoring and user feedback sessions (Winkler & Söllner, 2018).

Using a chatbot can help ensure that the information provided to the learners is consistent and available when and where it is required, including assessment criteria, due dates and location

of recommended resources (Cunningham-Nelson et al., 2019). The way a chatbot communicates with learners is synchronized, which makes it easy to react to individual intent. In addition, chatbots utilized as formative tools have an additional impact on engagement indicators and task completion (Winkler & Söllner, 2018). Sandu and Gide (2019) posit that various functions that can be performed by a chatbot in the area of learning include FAQs (Frequently Asked Questions), administrative and management tasks, student mentoring, motivation, student learning assessments, simulations, training specific skills and abilities, and providing reflection and metacognitive strategies. Figure 2.2 explains how the selection is made based on user input.

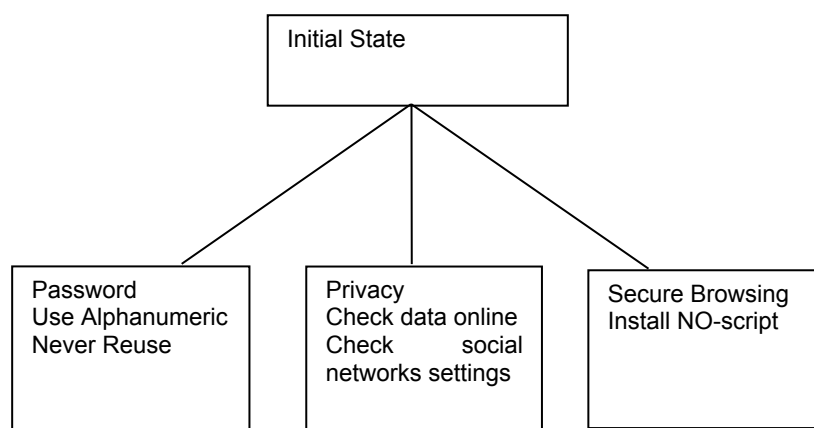


Figure 2.2: Chatbot topic selection based on user's input adapted from (Ignatov et al., 2014)

A crucial mechanism of conversational AI is the chatbot. This item provides natural guidance and performs design concentrates on going about as a savvy and effective partner. The bot uses rationale to determine client requests and interface with big corporate frameworks to achieve the desired end results (Sivaranjani, 2020). Candello et al. (2019) believe that chatbots will be placed in spaces of social interaction, informal learning, and entertainment; consequently, those machines should be trained for such. Chatbots aim to amplify entrants' literacy using motivational and educational messages and reinforce users' reasons (Gabrielli, Marie & Corte, 2018). This approach relies heavily on encouragement and motivational techniques to create effective suggestions and recommendations that consider users' desire to change. The benefits of this approach are, improved productivity, communication, learning, efficient teaching assistance, and minimized ambiguity from interaction (Sandu & Gide, 2019).

Studies have proved that chatbots improve task adherence. If users trust a bot, they engage in interactions willingly and thus increase the number of utterances in multi-party dialogues (Coperich, Cudney & Nembhard, 2017; Winkler & Söllner, 2018; Nordberg et al., 2019). Chatbot typology, chatbots with coaching-related roles usually have a chatbot-driven conversation approach and long-term relations. This essentially means a chatbot is in charge of the communication, and a chatbot and user(s) are expected to have a series of interactions over time (Coperich, Cudney & Nembhard, 2017). ML techniques have various designs, such as supervised, unsupervised, and reinforcement learning. Each ML technique is achieved by using various algorithms. Supervised learning is more suitable for tasks such as classifying user intents from user utterances. Unsupervised clustering algorithms are ideal for finding clusters of users based on their conversational behaviours and for learning efficient and optimal conversation behaviours (i.e., what should the bot say now?). Reinforcement learning algorithms are more suitable (Oduntan & Adegboye, 2017).

2.7 Chatbot Implementation

Java programming language is widely used to implement a chatbot (Dahiya, 2017). Especially Java applets, applets are specifically utilized for the ease of creating the dialogue box needed for the conversation between the user and a chatbot. What is required from the chatbot and the audience to whom the chatbot has created needs to be examined and analysed carefully? A chatbot should be tailored to suit the user's needs and address the relevant questions, or the responses of a typical user will yield a more human-like impact. Enabling a chatbot to accomplish such an impact will also enhance its overall intention and the experience of users engaging with the chatbot (Kowalski et al., 2013, Brandtzaeg & Følstad, 2017).

Natural Language Parser (NLP) records user requests and translates them into the conversation engine's programming language. NLP helps to determine the syntax and structure of the language. The conversation engine then analyses the question and redirects it to the backend. The backend is attached to one or more databases (DB) or information systems (IS) that provide the request to the relevant query (Jaf & Calder, 2019). Chatbots and language parsers rely on semantic patterns and keywords to examine users' queries and edit them to ensure accuracy. Chatbots recognise patterns or regularities by matching databases stored in

the backend and combining them. This method is often referred to as machine learning. Moreover, various chatbots employ the technique of deep learning, a subcategory of machine learning (Zumstein & Hundertmark, 2018a). Cahn (2017) explains that the objectives of natural language processing (NLP) are to convert the unstructured output of the ASR to a structured representation of the text that contains spoken language understanding (SLU) or, in the case of text input, natural language understanding (NLU). For a chatbot to be able to manipulate the text resulting from speech recognition and speech-to-text conversion, specific toolkits are required to arrange the text into sentences and then split them into words to facilitate semantic and meaning extraction. One of these toolkits is the widely used The Natural Language ToolKit (NLTK), a free plugin for Python. NLTK is a set of modules, tutorials, and open-source exercises that cover Natural Language Processing symbolically and statistically (Abdul-Kader, 2015, Dahiya, 2017).

Ghose and Barua (2017) note that writing Artificial Intelligence Markup Language (AIML) requires a technique, and developing a robot character, especially when writing default responses. Augello, Pilato, Machi and Gaglio (2012); Cahn (2017) note that the Artificial Intelligence Markup Language Knowledge Base (AIMLKB) is a pyramid where it is possible to identify four main types of categories:

Atomic, specific categories that predict a predetermined set of questions and respective answers; these categories can be manually created by the botmaster or automatically created by querying the ontology (using the AIML Bootstrap module) (Suta et al., 2020).

Default categories with wildcards inside their pattern and standard AIML tags in the template (Ghose & Barua, 2017).

Ontology-based, categories can have particular tags introduced to interact with the ontology. The pattern can contain wildcards that can match ontology concepts (Chan & De Souza, 2017).

Ultimate default, a category containing only a wildcard in its pattern. It corresponds with any user input; the template implements the module E-SRAI to perform the query's processing and uses its result to call the pattern matching again (Suta et al., 2020).

Paikari and Van Der Hoek (2018) state that many chatbots operate unidirectionally instead of engaging in an entire conversation.

Input chatbots often monitor a communication channel for specific words or phrases that a developer may enter as the trigger and invoke different actions depending on the specific words or phrases. These chatbots do their work silently.

Output chatbots operate by inserting content into communication without receiving instruction or input that tells them what to do; these chatbots are usually externally triggered and report on important events elsewhere.

Bi-directional chatbots receive input and produce output on the communication channel. These may be simple trigger-response interactions but also approach real conversations.

2.8 The gap in the literature

2.8.1 Introduction

This section will discuss how the systematic literature review assisted the researcher in examining and analysing current literature to identify the gap in the body of knowledge. The threat of cybercrime has generated a great deal of interest in cyber security. Institutions invest heavily in high-tech security solutions to prevent malicious online attacks from the ever-evolving range of current and potential future threats. Organisations spend huge sums of money on high-end security equipment. However, they often underestimate the risk of the insider threat created by their own users (Bogataj, Aver & Bogata, 2016). Research has shown that the main culprit with regard to the internal threat is often the employees. Phishing attempts are high on the list of less technical attacks that target humans. Also, the research shows that a lack of adherence to password policy is prevalent among users: weak or reused passwords and bad password-sharing practices (Gundu & Flowerday, 2013; Bada & Nurse, 2019).

Moreover, socially engineered attacks are directly linked to phishing scams (Al-Shanfari, Yassin & Abdullah, 2020). Marble et al. (2015); Linkov et al. (2019) believe the human element of cyber security is fast proving to be a major source of security breaches. Hackers use low-tech attacks like social engineering, focusing more on exploiting human vulnerabilities than using sophisticated techniques to gain information or breach the system (Conteh & Schmick, 2016). Lack of training and awareness, user naivety and negligence have been cited as major contributing factors towards security breaches aimed at users (Al-Darwish & Choe, 2019).

Cyber-security protects IT equipment, resources, and users against external threats. However, insider threat is equally damaging if neglected. (Tam & Jones, 2019). Furthermore, the human factor in IT security is one element that is always overlooked until a user clicks on a malicious link, opens an infected attachment, plugs in a USB that contains malware or a naïve user that's eager to help and does not want to get on the wrong side of the superiors provides sensitive information to hackers without checking with the IT team first. There are numerous occasions where our human nature supersedes logic, and IT security is one of them (Luh et al., 2017). One of the major reasons a company gets breached is due to their frontline users and their level of security awareness being weak (Bhatia, Behal, & Ahmed, 2018). In other words, the human element as the first line of defence is a crucial aspect of cyber security.

Another point to consider is that cybercrime carries huge financial damage and negatively impacts the organisation's reputation, shareholders, and customers. (Eubanks, 2017). Luh et al. (2017) advise that users' knowledge and awareness are vital to the organisation's security. Hence it should not be solely the responsibility of the IT department to raise awareness and understanding. Employees pose a serious threat to security, and the human factor is still a major challenge for end users and IT professionals (Hills & Anjali, 2017). Investing in effective security methods can yield positive returns when the users understand their critical roles and responsibilities in securing cyber networks. Exploiting human vulnerabilities using social engineering still carries a considerable risk for organisations. Judging by the escalating number of security attacks on human vulnerabilities, it is quite evident that there is a need to raise awareness among users and strengthen the first line of defence, which are humans. Another causal relationship between cyber security attacks and human vulnerabilities stems from humans' trusting nature, making humans a prime target for online hackers who exploit these vulnerabilities (Kaushalya, Randeniya & Liyanage 2018).

The motivation to carry out this study was triggered by the constant flux of online attacks that target government institutions. In this regard, cyber-attacks have been exploiting human weaknesses and naivety because outsourced security services put more emphasis on securing the infrastructure and, in the process, overlook human weaknesses. Research has shown that

over 35% of cyber-attacks are directly linked to human weaknesses. In addition, 50% of major attacks are due to human errors (Evans et al., 2016).

2.8.2 Method

The review method adopted a systematic approach incorporating review protocol, research question identification, search strategy, study selection and data extraction.

2.8.3 Review Protocol

Review protocol helps the researcher avoid prejudice and guards against negatively influencing the objectives and goals of the systematic review process.

2.8.4 Research Question

The research question forms a major building block and shapes the structure of SR. Based on the abovementioned concerns, this study aims to examine human vulnerabilities in cyber security in government Institutions or entities. In pursuance of this aim, the following SR questions are investigated:

RQ1.What solutions are available to counter or neutralize security threats that target human vulnerabilities in government entities?

RQ2.What are the key strengths and weaknesses of the current solutions?

RQ3.What are the implications of the current solutions?

2.8.5 Search Strategy

To determine the gap in the literature, the search strategy involves devising a systematic search, identifying key text that should form part of the search criteria, identifying digital libraries to be used and fine-tuning the search process. The investigation was conducted using the following digital libraries: IEEE Xplore, Google Scholar, and Science Direct between 2010 and 2019. The Boolean operators AND and OR were used in the search strategy to form a string of keywords that are relevant to the literature. Cybersecurity attacks that take advantage of human vulnerabilities though not new in the realm of Cybercrime, have become popular in recent years. Subsequently, the search was limited from 2010 till to date. The keywords had to relate to human vulnerabilities in cyber security in government entities. Therefore, the search focused

on keywords such as the human factor in IT security, human vulnerabilities in cyber-attack, the impact of human nature in cyber security, social engineering, and negligence of users. After carefully sifting through many papers, only a handful proved relevant to the study.

2.8.6 Study Selection

The process of Study Selection deals with separating relevant studies from irrelevant ones. That means systematically examining the contents (titles, abstracts, conclusions, and full texts) of the gathered studies to ensure their relevance.

2.8.7 Inclusion Criteria

IC1. Current studies on the subjects of social engineering and the human factor in cyber security.

IC2. Studies that showed empirical relevance.

IC3. Papers were written in English

Table 2.2: List of studies

Source	Number of studies	Type	Number of studies with relevance to the search title	Studies that showed relevance to the full text of the research
IEEE	30	Journal	20	2
Xplore Google Scholar	40	Journal	35	2
Science Direct	2	Conference	2	1

2.8.8 Exclusion Criteria

EC1. Studies conducted before the year 2010 EC2. Studies not written in the English language

2.8.9 Study quality assessment

The importance of the assessment is to ascertain the equality of all the studies selected and apportion a certain score that determines the relevance towards the study. See below for how the scores should be allocated. The scores basically measure the relevance of the study and if it should be accepted or rejected. Studies with a mark below the average were rejected, and those that obtained scores above the average.

2.8.10 Quality Score

The following scores are used to determine the validity of the articles.

9 - 10 Very high

6 - 8 High

4 - 5 Medium

0 - 3 Low

2.8.11 Results

A combination of tools and techniques, such as tables and charts, provides a synopsis of SR outcomes. This allows the researcher to present the results in tables or charts. At this stage of the SR, all the questions that form part of the research question are answered in a systematic manner.

Table 2.3: Quality Evaluation.

Study	Author	Quality Score
Ignorance to awareness: Towards an information security awareness process.	Gundu, Flowerday	9
End-user Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study	Bauer, Bernroider, Chudzikowski	8
Impact of Security Awareness Training Components on Security Effectiveness: Research Findings	Quagliata	7
Training Programs to Increase Cyber-security Awareness and Compliance in Non-profits, University of Oregon	Ray	6
Towards Detecting and Classifying Malicious URLs Using Deep Learning	Curran	6

2.8.12 Data Extraction

Data extraction form gathers and analyses all the papers that the researcher obtained during the selection of primary studies.

Table 2.4: Selection of Primary Studies.

Publication Name	Author	Year	Paper Number
Impact of Security Awareness Training Components on Security Effectiveness: Research Findings	Quagliata	2012	1
End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study	Bauer, Bernroider, Chudzikowski	2013	2
Ignorance to awareness: Towards an information security awareness process	Gundu, Flowerday	2013	3
Training Programs to Increase Cyber-security Awareness and Compliance in Non-profits	Ray	2014	4
Towards Detecting and Classifying Malicious URLs Using Deep Learning	Curran	2018	5

2.8.13 SR Summarization

This is a summary of the papers that formed part of the review. Previous studies on cyber security attacks have consistently shown that the human factor is very important in cyber security. Often organisations see social engineering scams that aim to extract information from employees and then use that information to gain access to the organization. Most organisations underestimate the threat that is posed by social engineering. However, it can easily be exploited as it capitalizes on human psychology rather than the technical barricades surrounding the complete system (Al-Darwish & Choe, 2019).

RQ1 What solutions are available to counter or neutralize security threats that target human vulnerabilities in government entities? This question outlines the details of current solutions used to empower users against cyber-attacks. The selected studies identify training and awareness as the current solutions. The current solutions are further sub-categorized as below:

1. Conventional Delivery Methods
2. Instructor-led Delivery Methods
3. Online Delivery Methods

Table 2.5: Delivery Methods

Solution	Method	Authors
1	Posters, stickers, leaflets, Employee newspaper	Bauer, Bernroider, Chudzikowski (2013), Ray (2014).
2	Formal presentations and training	Bauer, Bernroider, Chudzikowski (2013), Quagliata (2012). Curran (2018), Gungu, Flowerday (2013),
3	Online based training Security alert messages (e.g., screensavers, pre-login messages, email messages) Mobile learning platforms (e.g. social media) Game-based delivery methods	Bauer, Bernroider, Chudzikowski (2013), Gundu, Flowerday (2013), Quagliata (2012).

RQ2 What are the key strengths and weaknesses of the current solutions?

Classroom Strengths: allows users to interact with the instructor; at face value, it appears to be the ideal method. It adds a 'human touch' and personal interaction to the method of training, which encourages interaction among users and facilitators. The learning process can be adjusted according to the needs of a group; specific aspects can be debated, and queries and uncertainties can be dealt with immediately during the session. Topics that need more clarification can be reviewed, and users have the luxury of interacting with their peers and sharing their experiences (Johnson, 2017).

Classroom Weaknesses: information overload and users cannot pace themselves. In contrast, the online approach offers flexibility as the material can be accessed at the user's convenience without feeling overwhelmed. In class, the workload and amount of time allocated to the course dictate the rhythm, and learners are required to adjust to the pace. Another downside of a classroom approach is the need to attend classes, a significant challenge for an organization with offices in other countries or regions and employees that are not office-bound (Gundu & Flowerday, 2013; Bada & Nurse, 2019).

Online Strengths: offers adaptability; course material can be accessed at the user's convenience. Learning becomes accessible beyond physical location boundaries; learners can listen to instructors, keep track of course modules, launch coursework sessions, work on exercises, and participate in virtual labs, provided there is a computer and Internet connection. This is even more ideal for teleworkers as it does not require attendance and can be less expensive because it eliminates the need to provide training at various sites. In addition, users can pace themselves and adjust according to the demands of the topic. Users can also schedule courses at their convenience (Sabillon et al., 2017).

An online solution can also assist the organization's IT security team in measuring the users' preparedness. In addition, it is easy to track and report on the training status. Built-in simulated phishing attacks capability helps users spot phishing attacks and aids the organization gather results. Analysis and reporting capabilities are important when arranging a rundown for management and pinpointing weaknesses and issues to address quickly. Comprehensive customization techniques are required to adjust the training to the demands of each section in the organization and evolving requirements (Curran, 2018).

Online Weaknesses: it demands much input from the users and requires self-motivation and the desire to go the extra mile if the topic is unclear. This places more burden on the users to be self-driven and responsible for their own education. Online methods, unfortunately, cannot address matters as they arise because instructors are usually unavailable in real-time. The online method offers users limited support via emails and chats. However, it is somewhat challenging to have a synchronous interaction with trainers and facilitators in different places at different times. Learners must be able to apply what is learned to specific examples derived from their experience. The major downside of online training is the lack of peer-to-peer and instructor interaction. Moreover, course material cannot be tailored to the specific needs of different trainees. In a class approach, the facilitator can adapt the training as the need arises and can prepare lessons to suit the targeted audience. However, online courses are usually more generic and do not cater to a specific audience's needs. (Gundu & Flowerday, 2013; Bada & Nurse, 2019).

Table 2.6: Strengths and Weaknesses adapted from (Bauer, Bernroider & Chudzikowski, 2013)

Delivery Method	Strength	Weakness
Conventional delivery methods	Periodic information Security reinforcement Bulk messaging Easy to track	Messages likely to be overlooked It may be perceived as spam
Instructor-led delivery methods	A facilitator can quickly pick up non-verbal cues Adjust training approach Questions and queries can be addressed in real-time	Cost It does not appeal to many users It relies heavily on the facilitator's knowledge and experience
Online delivery methods	Only effective if learners put in the needed effort Less expensive Adaptable models that allow learners to pace themselves Training is consistent throughout the organization Easily noticeable, which makes them a more suitable channel for delivering critical security awareness messages Monitoring of progress It can be challenging, motivating and engaging	Less attractive due to volumes of email and spam Difficult to measure the actual impact Users often do not in the necessary effort due to a lack of supervision Becomes unvarying Fails to challenge users It does not offer interaction between users and instructor Isolates users Complex implementation It does not address the security challenges of a specific organisation

RQ3 What are the implications of the current solutions?

This question looks at the key strengths and weaknesses of each solution that was examined in RQ2. What are the strengths and weaknesses of the current Information Security Delivery Methods? We looked at solutions that are widely used in the IT security domain. Training and awareness are backed by many studies that were examined in RQ2. Both studies have proved effective in providing the necessary training and awareness. The classroom-based solution enables users to interact with the instructor and discuss specific topics where there is a need for clarification of certain terms. However, the solution can overwhelm users with information, as they cannot pace themselves. Therefore, in cases where time is a limitation, the classroom-based solution seems to underperform. On the other hand, online training solution is flexible and can transcend classroom-based boundaries. The online solution is ideal for the distributed workforce; it does not require a physical location. Also, it allows users to pace themselves and take the training at their convenience (Aldawood & Skinner, 2018).

Online training also provides simulated online attacks that replicate real-world online attacks. The drawback of online training is that; it is more demanding on the users. Users need to be self-motivated and do their own research, which puts more pressure on them. Studies have shown that no method is better than the other. In most cases, the type of organization, the culture and the size determine which method best fits the organization. In the case where you have distributed users, an online approach might be more suitable, and in the case where physical location is not a challenge adopting a classroom-based might be more appropriate. The studies further proved that combining the solutions can yield better results than employing a specific solution (Quagliata, 2012; Johnson, 2017). Gundu and Flowerday (2013); Curran (2018) argue that ongoing awareness and training programs are crucial to the success of information security compliance. Quagliata (2012); Bada et al. (2019) highlight the lack of innovative methods to monitor and enforce information security compliance.

2.8.14 Summary

A systematic literature review on human vulnerabilities in cyber security was conducted to examine the current cybercrime solutions. We selected and analyzed 50 studies between the years 2010 – 2019. The next step was to analyze methods and techniques to summarize primary studies. An assessment of the proposed solutions was done in line with the set goals of the study. In addition, a comparison of the current solutions was also done. Then finally, the strengths and weaknesses of the solutions were analyzed. The study has shown that, when deciding on the type of solution to deploy, the schedule, needs and size of the organization

always influence the decision. The online solution is more suitable for offsite users, and the classroom-based solution is more suitable for onsite training. Therefore, in most situations, a hybrid solution is preferred because it blends the two solutions (Curran, 2018; Azmi, Tibben, & Win, 2018). Compliance is a huge part of Information Security. However, there seems to be little or no research on this important area of cyber security. It is therefore suggested that the research should be conducted on effective training solutions that can enforce and monitor ongoing compliance.

2.8.15 Limitations and Recommendations

RQ2 analyzed two current methods used in the fight against cybercrime, and the strengths and weaknesses of each approach were analyzed in detail. A hybrid approach has been recommended to essentially combine the benefits of each method and take advantage of their individual strength, and, in the process, eliminate the weakness of the isolated approach. Studies have shown that much work still needs to be done around compliance.

2.8.16 Conclusion

A systematic literature review on human vulnerabilities in cyber security was conducted to examine cybercrime solutions. Compliance is a huge part of Information Security. However, there seems to be little or no research on this important area of cybersecurity. Therefore, the research should be conducted on effective training solutions that enforce ongoing compliance.

2.9 Summary

This chapter discussed literature in the user security domain. It examined the security behaviour of users extensively, factors that contribute to the behaviour of users, consequences of non-compliance and improper security conduct, approaches that foster compliance, non-compliance factors, acceptable user security behaviour, the impact of recognizing compliance and punishing non-compliance as well as various solutions that can improve the behaviour users. The chapter also looked at the role of a chatbot, specifically the basic theory behind bots, various types of chatbots, uses of chatbots, chatbot framework, the role of chatbots in training and education, and implementation of chatbots.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter gives a detailed account of the study's methods to fulfil this research project's requirements. The chapter will also cover the following topics: research design, experimental research, properties of experimental research, ensuring quality in experimental studies, experiences and motivation, literature review analysis, hypothesis, research methodology and strategy, conceptual framework, data collection, and data analysis and limitations of the study.

3.2 Research Paradigm

Taylor and Medina (2011) define a paradigm as an overarching set of principles, ideology, or framework that informs research and practice in a specific discipline. The positivist paradigm of investigating social phenomena emanates from the philosophical concepts of the French Philosopher August Comte. He argued that through observation and reasoning, we are able to understand human conduct; true knowledge is rooted in the experience of the senses and can be attained through observation and experiment (Antwi & Hamza, 2015).

Positivists maintain that the objective approach to developing knowledge should not be determined by the researcher's input or participants' influence. To aptly develop knowledge, participants and the researcher must be completely separated. Positivism is based on hypothetico-deductive reasoning to prove theoretical hypotheses that are usually quantitative, where a causal relationship between independent and dependent variables can be established (Park, Lars & Artino, 2019). Positivism is concerned with objectivity and accepting or rejecting the hypothesis (Gemma, 2018). Figure 3.1 provides a pictorial description of the positivism paradigm.

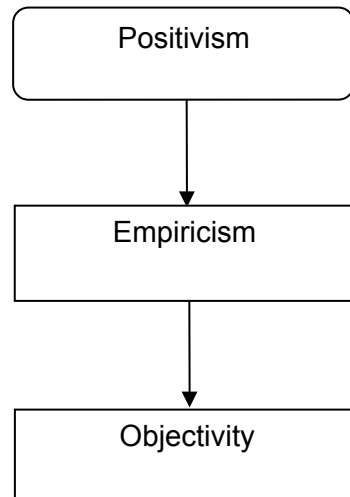


Figure 3.1: Philosophical positivism paradigm adapted from (Gemma, 2018)

3.3 Research Design

Research design is a research method designed to address research questions and problems. The research design details the plan of action of what the researcher will undertake, from developing a hypothesis to finalising data analysis. (Kumar, 2011). The research design of this study is experimental, and therefore, it will adopt the principles of an experimental research study. Apuke (2017) defines experimental research design as an outline that helps a researcher test a hypothesis to deduce the relationship between dependent and independent variables.

3.3.1 Experimental Research

Experimental research is quantitative, and it can be defined as an experiment that is conducted in a controlled setting to illustrate a known fact or to scrutinize and validate the hypothesis (Muijs, 2015). Mitchell and Jolley (2010) argue that an experiment requires two groups (control and experimental) that should have similar traits before the start of the experiment. However, throughout the experiment, one group (experimental) will receive treatment or intervention that is different from the other (control).

3.3.2 Properties of experimental research

Experimental research requires that certain variables are controlled while others are manipulated to test the hypothesis (Akhtar, 2016). The experimental study aims to establish the causal relationship between the dependent and independent variables (Asenahabi, 2019).

According to Baker (2019), for a research study to be regarded as experimental, it must have intervention treatment, control of extraneous variables and randomization.

1. Intervention is applied to the experimental group or to influence the independent variable.
2. Control of extraneous variables in the control group enables the researcher to measure the impact of the treatment on the experimental group.
3. Randomization means participants are assigned to different groups randomly.

Experimental studies are characterized by three distinct features: control over the independent variable, random assignment of units of analysis and nuisance variables. Experimental research emphasizes setting control and focuses on the variables of interest (Wellman, Kruger & Mitchell, 2005). Having total control of the environment allows us to have a clear perspective on the cause (intervention) and effects. The other important aspect of the control feature is the elimination of experimenter bias, i.e., it ensures that participants receive the same treatment (Muijs, 2015). Welman et al. (2005) add that total control enables us to manipulate the independent variable. In order to determine to which group will the participants be assigned? We make use of random assignments. In a random assignment, all participants have a fair chance of getting selected for the treatment or non-treatment group (Mitchell & Jolley, 2010). It is worth noting that random assignment does not refer to how participants are elicited but how they are assigned to various groups. Random assignment can be achieved through a coin toss or a table of random numbers (Welman et al., 2005).

A variety of variables that were not determined in the hypothesis can impact the dependent variable. The impact of these nuisance variables may weaken or strengthen the relationship between independent and dependent variables (Kumar, 2011). Welman et al. (2005) argue that experimental research is primarily designed to eliminate nuisance variables and ensure that the only difference between the groups is based on the independent variable in question. Conducting an appropriate literature review is necessary for managing the nuisance variable as it helps pinpoint previous studies that have covered it. The most effective approach to dealing with the nuisance variable is to add it to the design as an additional independent variable. Also, ensuring that all the variables among the groups are the same except for the independent variable can increase the chances of controlling the nuisance variable.

3.3.3 Ensuring quality in experimental studies

The quality of the research design can be determined based on four fundamental aspects: internal validity, external validity, construct validity, and statistical conclusion validity. Internal validity seeks to establish the impact of change in a dependent variable, i.e., is the change due to the relevant hypothesized independent variable or is it due to a nuisance variable? External validity, sometimes called generalizability, aims to ascertain the generalizability of the observed phenomenon related to the entire population (Bhattacharjee, 2012). Construct validity ensures that the chosen measurement scale is intended to assess the theoretical construct. Statistical conclusion establishes the degree of validity of the statistical methods used in the study. Muijs (2015) posits that validity, reliability, and generalizability are fundamental to the quality of an experimental study. According to Kumar (2011), validity ensures that an instrument can measure what it intends to measure.

The best research design should display significant levels of validity (Bhattacharjee, 2012). With that said, Mitchell and Jolley (2010) advise on the following caveats regarding validity: firstly, you need to consider practicality over validity, which means the measure must be affordable, and you must be able to control it. Secondly, ethical considerations should override validity, meaning that in the event the appropriate measure is likely to compromise or put participants in danger, then it should not be used. Thirdly the measure's primary aim is more important than its validity. The measure should address the research question or hypothesis. Reliability refers to the dependability and consistency concerning the measure of a construct, i.e., if the same construct is measured repeatedly, it should give us consistent results, particularly if there is no change to the underlying phenomenon. Reliability is concerned with eliminating measurement errors from the results (Muijs, 2015). Marczyk et al. (2005) emphasize using reliable measures to attain reliability and reduce random variability in experimental studies. In experimental studies, sampling is key to generalizing the results to the entire population (Muijs, 2015). The sample should represent the entire population for a study to achieve generalizability. In addition, when it comes to the size of the sample, it is worth noting that a larger sample size will reduce the potential error of generalising to the population (Welman et al., 2005).

3.4 Research process

Figure 3.2 outlines the step-by-step process of how the research for this study was conducted.

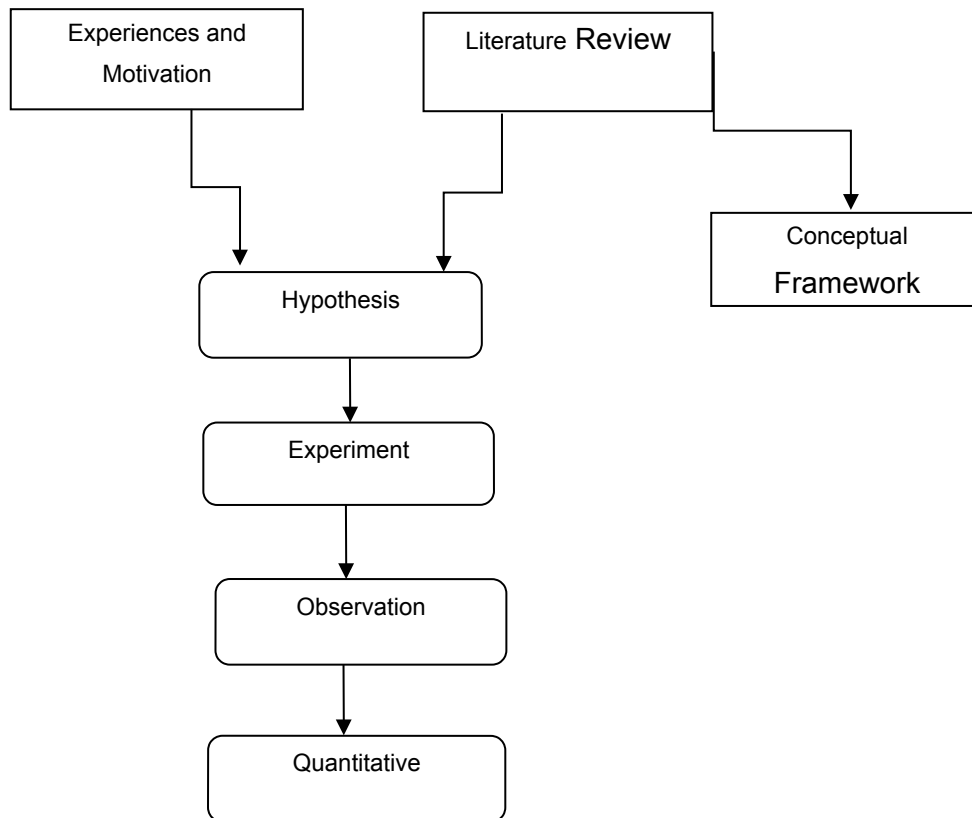


Figure 3.2: Research process

3.4.1 Experiences

User compliance is one aspect of ISA that presents an ongoing challenge in improving information security compliance levels. The perception that an information security policy is a document that needs to be signed periodically inadvertently creates an impression that information security compliance is not intricately linked with the business strategy, and thus, the contents of the information security policy need not be carried out continuously.

3.4.2 Motivation

The motivation behind the study was to encourage security compliance without the need to reward compliance or punish non-compliance. Security compliance should be practised at all times; therefore, using a chatbot to remind users about the contents of security policy constantly can improve compliance levels. Another motivating factor was to see a positive attitude towards compliance. Users view security as an inhibitor of productivity or a time-consuming task. Organisations have tried various approaches to improve compliance levels, such as rewarding compliance and punishing non-compliance. However, these approaches have proved not enough to address the issue of ongoing compliance. Both methods are reactive, and thus their impact is not far-reaching.

3.4.3 Literature review analysis

The literature review has highlighted the importance of awareness and training in ISA. However, it has become evident that maintaining high levels of compliance is nearly impossible to achieve. Once users complete the training, it becomes apparent that they are practically left on their own devices. The hope is that awareness and training will equip them with all the necessary tools for their daily security encounters. This has exposed a gap in the current approaches. Literature has proved that the cost of compliance is too much of a burden to bear for employees. Striking a balance between productivity and compliance is not easily attainable. Research has proved that the former will always take precedence when users are faced with a quandary of choosing between productivity and compliance. Information security awareness and training cannot afford to be static due to the dynamic nature of security attacks. Therefore, viewing the training material only during the annual training and compliance reviews cannot quell non-compliance behaviour. This highlights a need for a mechanism that can offer ongoing compliance support. Incentivizing compliance behaviour and penalizing non-compliance behaviour have been cited by many studies. However, research has shown that the latter creates fear among employees. Also, incentivizing compliant behaviour has not produced the envisaged results. Educational chatbots are gaining momentum, and the adoption rate is gradually increasing. These chatbots have become ubiquitous in the eLearning space. These chatbots can provide auxiliary features that complement information security awareness and training.

3.4.4 Hypothesis

Fellows and Liu (2015) define a hypothesis as a belief held without proof or a proposition made, as a starting point for further investigation, from known facts. It is a statement about the

anticipated relationship between two or more elements (El Hadi et al., 2011). A research hypothesis should have the independent and dependent variables distinctly stated. (Bhattacharjee 2012). Marczyk, DeMatteo, and Festinger (2005) add that a hypothesis must be able to formulate predictions that can be tested to determine if they uphold or oppose the hypothesis. The independent variables for this research hypothesis are strong passwords, attachments and scan devices, and the dependent variables are compliance and non-compliance. The hypothesis will test the causal relationship between the independent and dependent variables. The hypothesis for this research study is that users who receive a constant reminder about the contents of ISP have a higher information security compliance behaviour than users without any form of reminder.

3.4.4.1 Difference between research hypothesis and research question

The difference between a hypothesis and a research question is based on the fact that a research question is always expressed as a question. In contrast, the hypothesis is expressed as a statement. The hypothesis is more suitable for studies that employ explanatory and deductive research. Hypotheses are usually stated in a form that predicts a difference between two groups regarding some variable (Wellman et al., 2005).

3.4.4.2 Type I and Type II Errors

Muijs (2015) states that type I errors occur when the null hypothesis is incorrectly refuted. In contrast, type II error happens when a null hypothesis is wrongly accepted (Kumar, 2011). In dealing with a type I error, the significance level or the p-value has been set at $p \leq 0.05$. This p-value indicates that the chances of erroneously refuting the null hypothesis or encountering a type I error are less than or equal to 5% (Bhattacharjee 2012). To reduce the chances of making a type II error, a researcher can increase the sample size (Chaudhury & Banerjee, 2009). Louanglath (2017) opines that a sample size between 30-200 is regarded as a decent minimum for research studies.

3.4.5 Research Methodology and Strategy

The study is intended to ascertain if a constant monitoring approach can help improve information security compliance levels. The study will experiment with a chatbot to prove the hypothesized supposition. The methods that will be used in the study conform to the principles of quantitative research. A strong password, attachments and scan devices and encrypted files are all variables that will be measured in the study. The quantitative methodology provides a numerical rendition and manipulation of observations to describe and explain the phenomena

that are being observed (Sukamolson, 2007). Quantitative research mainly ensures that variables are quantified to determine the outcome. It utilizes numerical data, and with the aid of statistical methods, it can address questions like who, how much, what, when and how many (Apuke, 2017).

Quantitative research methodology can be described as the systematic empirical inquiry of discernible phenomena through statistical methods (Bhawna & Gobind, 2015). Apuke (2017) argues that in quantitative methodology, research data is collected, quantified and statistically analysed to refute or uphold the hypothesis. Quantitative research offers a more analytical perspective on research (Asenahabi, 2019). Quantitative research ensures the quantifiability of data and the generalizability of results obtained from a sample of the selected population (Macdonald & Headlam, 2011). El-Gohary (2010) postulates that quantitative research is based on the hypothesis that is deduced from a theory, and thus, quantitative tends to lean towards the deductive approach. The quantitative approach employs deductive reasoning as it seeks to explore regularities in human conduct. This is achieved by dividing the social world into empirical units called variables that can be portrayed in numerical order. The association between variables can be examined using statistical methods. This requires a researcher to introduce an intervention or treatment (Rahman, 2020). Table 3.1 describes the characteristics of quantitative research versus qualitative research.

Table 3.1: Characteristics of quantitative research versus qualitative research adapted from (Source: Guido, 2016)

	Quantitative Research	Qualitative Research
Orientation	Uses a deductive approach to test theory	Uses an inductive approach to generate theory
Epistemology	It is based on a positivist approach inherent in the natural science	It rejects positivism by relying on individual interpretation of social reality
Ontology	Objectivist in that social reality is regarded as an objective fact	Constructionists in that social reality are seen as a constantly shifting product of perception

Eyisi (2016), in his justification for using quantitative methods, points out that it is often easier to replicate quantitative studies because, to test a hypothesis, a researcher needs to follow specific guidelines and objectives. This means the tests can be easily replicated at any other location. Statistical-based evidence allows for the generalizability of research findings (McCusker & Gunaydin, 2016). Hypothetical inferences can be drawn from a series of data

analyses. Data collection and analysis follow a structured approach that deals with either experimental or nonexperimental methods of gathering numerical data and generalizing the analysed results to the research population. This approach conforms to the principles of the postpositivist paradigm (Asenahabi, 2019). Table 3.2 depicts a comparison of quantitative research and qualitative research.

Table 3.2: Comparison of quantitative and qualitative research studies adapted from (Mack et al., 2005)

	Quantitative	Qualitative
General framework	Aim to validate the hypotheses about phenomena Devices used to obtain, and group answers are inflexible Employ highly structured methods such as questionnaires, surveys and structured observation	Aim to inspect phenomena Research tools are adaptable, repetitive approaches to obtaining and grouping answers to questions Use semi-structured methods such as in-depth interviews, focus groups and participant observation
Analytical objectives	To aggregate disparity To predict causal relationships To detail traits of a population	To detail disparity To detail and expound on relationships To detail individual experiences To detail group norms
Question format	Closed-ended	Open-ended
Data format	Numerical-based (answers are allocated numerical values)	Text-based (acquired from audio tapes, video tapes and field notes)
Results	Statistical	Interpretive
Flexibility in study design	The design is consistent from start to finish Participants' answers do not control how the researcher structures the questions Study design relies on statistical deductions and circumstances	The study maintains flexibility when it comes to the addition, execution, or wording of particular interview questions Participants' answers influence the researcher's questioning approach The repetitive nature of the design allows the researcher to adapt the research questions and data collection accordingly

3.4.5.1 Research Approach

This research study is deductive in its approach and therefore follows the principles of the deductive research method. The deductive approach starts with an accepted theory, and the theory, a hypothesis, is derived, tested, and revised (Woiceshyn & Daellenbach, 2018). The deductive research approach moves from supposition(s), a widely accepted assertion, to a conclusive statement. This approach follows a top-down model from theory to observation. The theory informs the observational conclusions of this approach. The deductive approach starts from a widely accepted supposition to a specific conclusion (Malhotra, 2017). Park, Bahrudin and Han (2020), in their comparison of the two approaches, that is deductive approach and the inductive approach, argue that a constructivist paradigm guides the inductive research approach and is more about constructing theories. The inductive approach aims to reconstruct phenomena to acquire a new value and a clear understanding of phenomena. In comparison, the deductive approach conforms to the positivist paradigm for validating and generalising theories. This approach deals with numerical data and is more concerned with proving suppositions. The table below describes the comparison between the deductive approach and the inductive approach.

Table 3.3: Deductive versus Inductive approach adapted from (Burney & Saleem, 2008)

Deductive	Inductive
Theory	Observation
Hypothesis	Pattern
Observation	Tentative Hypothesis
Confirmation	Theory

3.4.5.2 Sampling

A sample is a small subset that represents the entire population (Rai & Thapa, 2015). Sampling is a method used to select a number of subsets representing a population being researched to observe the traits of the entire population (Sharma, 2017). Singh and Masuku (2013) define sampling as a technique used to select a smaller number of individuals with all the traits that can be generalized to the entire population. A population is a group of people or objects from which the research sample is identified. Taherdoost (2016). population refers to the entire set of

individuals that share similar qualities based on specific standards (Datta, 2018). Population Identification means identifying the population of interest that can help a researcher answer the research question or prove the hypothesis (Majid, 2018).

Sampling methods are often used in research to save time and reduce costs without compromising the study (Singh & Masuku, 2014). Taherdoost (2016) postulates that collecting data about the entire population is virtually impossible and researchers have limited time and resources to study the entire population. Hence there is a need for sampling. The application of sampling in a research study reduces the number of instances. The sample size is often determined by the following five study design parameters: minimum expected difference or also known as the effect size, estimated measurement variability, desired statistical power, significance criterion, and whether a one- or two-tailed statistical analysis is planned (Singh & Masuku, 2013). Wilson (2014) argues that sample size depends on the researcher's study methods and the desired outcome.

3.4.5.3 Types of Sampling Techniques

Probability sampling is a method that ensures all members of the population have an equal chance of being chosen. This method requires much work. Still, it has a high-level degree of accuracy. Non-probability sampling method relies heavily on judgement (Sharma, 2017). This method is not concerned with giving individual members of the population an equal chance to be selected (Ilker, Sulaiman & Rukayya, 2016). Table 3.3 provides a comparison between the probability sampling technique and the non-probability sampling technique.

Table 3.4: Difference between probability and non-probability sampling techniques adapted from (Datta, 2018)

	Probability Sampling Technique	Non-probability Sampling Technique
Requirement of resources	Resource heavy with regards to time, cost and efforts	Does not require too many resources
Selection of sample	Random and impartial	Non-random and subjective
Quality in reference	Generalizability is applied to the population	It cannot be generalized to the population
Best suited for research	That aims to discern a population	That aims to conceive an idea or concept
Applicable to the kind of population	Finite number elements which are precisely defined and have a specific category	Finite elements of which are infinite, which is a too general category, not quite precisely defined
Chances of errors and biases	Less prone to errors and biasness	Susceptible to systematic errors and biasness
Types	Simple random sampling Systematic random sampling Stratified random sampling Cluster sampling Multistage sampling	Volunteer sampling Convenient sampling Purposive sampling Quota sampling (proportional and non-proportional) Snowball sampling Matched sampling Genealogy based sampling

3.4.6 Conceptual framework

A conceptual framework is a structure that the researcher believes is more suitable to describe the step-by-step development of the phenomenon to be studied (Adom, Hussein & Agyem, 2018). The advantages of a conceptual framework, according to Leshem and Trafford (2007), are:

1. It presents relationships among concepts.
2. It reduces conceptual data into statements or models.
3. It elucidates theories that are critical to the research.
4. It provides a theoretical foundation to research design.
5. It explains theoretical links between present research, current theories, research design, interpretations of findings and conceptual conclusions.

The conceptual framework improves the distinctness of the research processes and enables self-audit capabilities that provide continuity and appropriateness toward research conclusions.

The conceptual framework approach of this study (Figure 3.3) shows how the experiment will be conducted. Users will be assigned to the control and the experimental groups, respectively. Both sets of users will receive training based on a password, phishing, and BYOD policies. Users from the control group will only be exposed to the training, and the users from the experimental group will also receive similar training. However, in the case of the experimental group, treatment will also be administered, and in this study, the treatment will be a chatbot. A chatbot will proactively remind users about the password policy, phishing, and BYOD content. Lastly, both groups will be assessed to measure the impact of training and treatment on compliance and non-compliance.

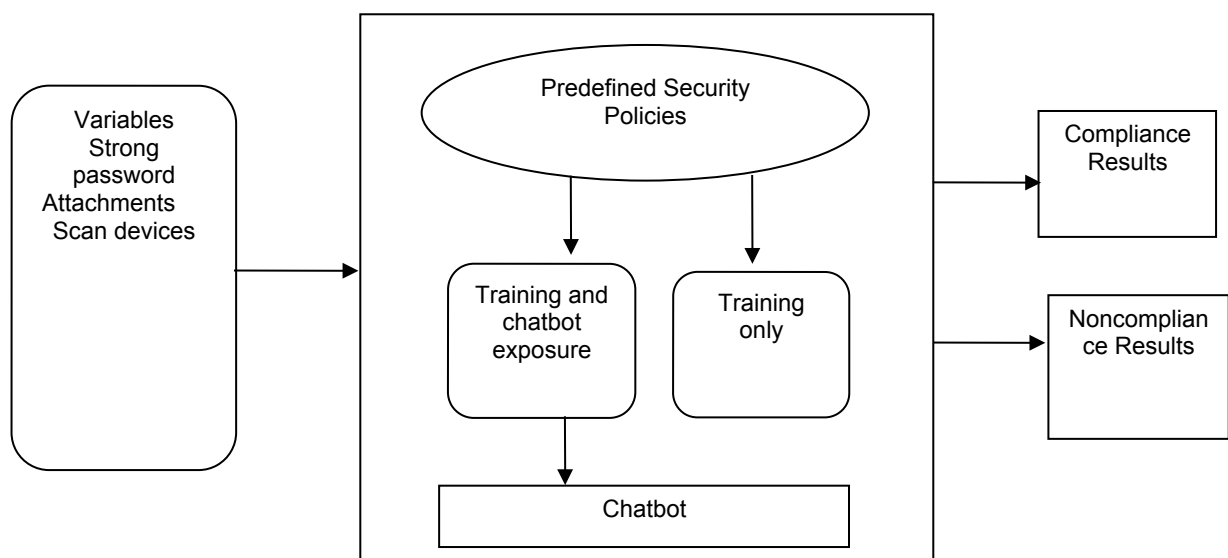


Figure 3.3: Conceptual framework

3.4.7 Data collection

This study aimed to determine the impact of a chatbot in enforcing ongoing user compliance in selected government entities. This meant that a chatbot would be employed to improve user compliance levels among government employees. The primary research data was collected from Department 1 and Department 2 in Cape Town. Ethical issues needed to be addressed before conducting the experiment; therefore, participants were advised about the ethical aspects of the study. Participants were also advised of the following: the study would not collect any personal data except for the gender and the age of the participants, participation in the study is completely voluntary, participants are free to withdraw from the study anytime, and the study will not offer any reward for participation, and lastly participants were informed that their participation would have a significant contribution towards the research and the findings. A

consent letter to collect data was elicited from the departments. An ethics approval letter was issued by the Office of the Research Committee (Appendix A). A participation letter inviting staff members to participate in the study was sent to all the potential participants.

Data collection was conducted on the 28th of May 2021 at Department 1's virtual resource centre in Cape Town. Another session was conducted online with Department 2 in Cape Town on the 23rd of August 2021. The invitation was extended to all the Strategic Support and Budget staff. A two-group experimental design guided the entire experimental process. A simple random sampling approach informed the process of selecting participants. Participants were divided into two groups and were randomly assigned to the groups respectively. The two groups were the control group and the experimental group. The control group consisted of participants who would not receive the treatment. The experimental group was manipulated to test the effect of the treatment. A non-participant observation approach was employed to gather primary data. The type of data collected during data collection was qualitative and analysed quantitatively. The data was collected from the control and experimental groups. The instrument that was used to capture and record data was a Microsoft Excel spreadsheet. The version of Excel was office 365 and was installed on Microsoft Windows 10 machines. A chatbot was the intervention during the experiment and was applied to the experimental group. The chatbot constantly reminded the experimental group how to create a strong password, deal with attachments, and scan external devices before they are used on the company network.

3.4.8 Data analysis

Data were analysed using quantitative methods of data analysis. Microsoft Excel was used to capture the data and analyse the results. The interpretation of the results was conducted using statistical measures. Kumar (2011) opines that statistics help us present the findings concisely and exactly. Descriptive statistics provided a detailed account of the results. Descriptive statistics summarise the sample data and report the observations made (Manju & Mathur, 2014). Podesva and Sharma (2013) note that descriptive statistics do not attempt to address the hypothesis. Descriptive statistics use central tendency and dispersion measures to describe a data set.

1. Mean: the average score of the data set
2. Median: middle value in the data set
3. Mode: value that appears the most in the data set
4. Range: the difference between the largest and the smallest value

5. Standard deviation: measures the spread of data in relation to the mean
6. Variance: a measure of variability from the mean
7. Standard error: a measure of disparity in the mean of the sample compared to the population mean.
8. Skewness: measures the symmetry of data distribution.
9. Kurtosis: describes the distribution of data.
10. Confidence interval: how confident are we that the results did not happen by chance?

Inferential statistics methods were used to prove the hypothesis. A t-test was used to test whether the results were statistically significant.

3.5 Limitations of the Study

Limitations of any research study are often associated with typical shortcomings of the specific method that are outside the researcher's responsibility. These are issues related to the research design, statistical methods restrictions, and funding restrictions. (Dimitrios & Fountouki, 2019). Quantitative research studies look to attain precise and definitive quantification that can be statistically analysed. However, just like any other research methodology, there are limitations that a researcher must explore and be acquainted with (Queirós, Faria & Almeida, 2017). Jerrim and De Vries (2015) note that quantitative research is a major contributor to the body of knowledge in the scientific research realm. This methodology is fraught with limitations that little is known or understood about, particularly by those who are not conversant with the methodology.

Quantitative studies find it difficult to measure the impact of treatment or educational significance (Rahman, 2020). Quantitative studies reveal behavioural patterns and trends but cannot explain why people behave in a particular way (Goertzen, 2017). Dimitrios and Fountouki (2019) believe that quantitative statistical methods can successfully establish relations amongst observed entities but cannot explain the cause-effect relationship. Akhtar (2016) argues that in experimental research studies, validity relies upon the similarities between the two groups that are being tested. Experimental research may be time-intensive, and thus the process of collecting data may demand extended periods of time (Goertzen, 2017). Camburn et al. (2016) are of the view that experimental research value in education is always under scrutiny because there is a belief that it cannot examine complicated causal hypotheses,

may not be able to generalize results to other situations, and the cost of undertaking experimental research may be too much. Rahman (2020) notes that quantitative studies tend to ignore participants' experiences and views in a highly restrained setting. Experimental research necessitates that a researcher is separated from the participants during data collection.

3.6 Summary

In this chapter, the research process was discussed broadly. The chapter covered research design, experimental research, experiences and motivation, literature review analysis, hypothesis, research methodology and strategy, conceptual framework, data collection, data analysis, and study limitations.

CHAPTER FOUR: EXPERIMENT PROCESS

4.1 Introduction

This chapter details the process that was followed when conducting the experiment of this research study. The chapter outlines the goals of the experiment, discusses the hypothesis and the variables, provides a brief background of the population that was used in the study, explains how the population for the study was identified, the sampling method that was used in the study, the instruments that were used to conduct the experiment and procedures that were followed during the experiment, tasks that were carried out to accomplish the experiment, a procedural task analysis of the series of tasks were outlined, the architectural design of the chatbot as well as the deviation from the protocol.

4.2 Goals of the Experiment

The goals of the experiment were as follows:

1. Train users about the contents of ISP. The objective is to train users on password policy, phishing, and BYOD. Upon completion of the training, users will be assessed to measure their performance.
2. Conduct the experiment using a chatbot as a treatment. The role of a chatbot will be to remind the experimental group about the training contents. This will allow us to administer the treatment.
3. Ascertain whether the use of chatbots can improve ISP compliance. Using a chatbot will ensure that users do not forget the ISP's contents and remain compliant.

4.3 Description of the hypothesis

The research hypothesis was the ultimate goal and the focal point of the research. It guided how the experiment was arranged. The experiment was designed to address the following hypothesis. Users who receive a constant reminder about the contents of ISP have a higher information security compliance behaviour than users without any form of reminder. A chatbot will serve as a treatment or constant reminder in this research. A chatbot will constantly remind users about the importance of creating a unique and strong password. For phishing, a chatbot

will remind users how to spot a phish and deal with it; for BYOD, a chatbot will remind users about the steps to take before using a personal device on the company network.

Null Hypotheses H_0 : There is no relation between user compliance and the use of chatbots.

Alternative Hypotheses

H_1 : There is a positive relationship between improved user password compliance behaviour and the use of chatbots.

H_2 : There is a strong relationship between users' ability to spot a phish and the use of chatbots.

H_3 : There is a positive relationship between users who scan their portable devices before using them on the company network and the use of chatbots.

According to Marczyk et al. (2005), the null hypothesis anticipates that there will be no difference among the observed groups. The null hypothesis affords a researcher the grounds to accept or dismiss the accepted hypothesis. The assumption is that any perceived difference is due to a sampling error, and the actual difference is zero (Singh, 2006).

Independent variables

The experiment will measure the following independent variables:

1. A strong password, this variable will be measured to establish if a chatbot is able to help users create a strong and unique password.
2. Attachments, with the aid of a chatbot, users should be able to spot a fake attachment or a spoofed email and URL.
3. Scan devices, a chatbot will remind users to scan devices for malicious programs and ensure that users check portable devices before using them on the company network.

The Independent variable, sometimes referred to as the intervention or experimental variable, is attentively exploited by a researcher under controlled circumstances to measure its impact on the dependent variable (Blaxter et al., 2012).

Dependent variables

The dependent variables for this research are, Compliance and Non-Compliance. The dependent variable is explored as the end results of an experiment or a research study (Salkind, 2012). A dependent variable is referred to as a "dependent" due to the influence the

independent variable has over it (Marczyk et al., 2005). If a user creates a strong password, that action will influence compliance. If a user does not scan a personal device, that will affect non-compliance. The independent variables will influence compliance and non-compliance. Users' responses to the treatment will either positively or negatively influence the dependent variables. The impact will measure the outcome of the experiment it will have on the dependent variables. If the user's behaviour is positive, the compliance-dependent variable will be influenced. If the user's behaviour is negative, the non-compliance dependent variable will be affected.

4.4 Population

The population for this study was drawn from Department 1 and Department 2 in Cape Town. Department 1 is responsible for developing sustainable integrated human settlements in the Western Cape. This means that the department is tasked with creating human settlements that allow its residents to access social and economic opportunities close to where they live. In the organisational structure, the department is headed by the Provincial Minister, the Head of the Department, Chief Directors and Directors. Figure 4.1 depicts the organisational structure for Department 1.

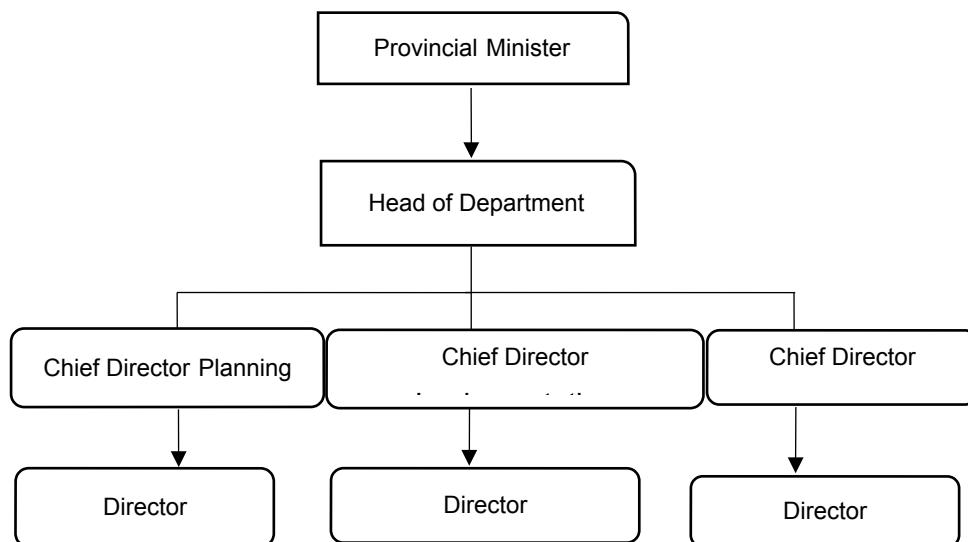


Figure 4.1: Organisational structure Department 1

Department 2 determines rate increases and indicates where money will be spent on programmes and services. As shown in figure 4.2, the department structure comprises the Executive Director, Director, Management and Financial Officers.

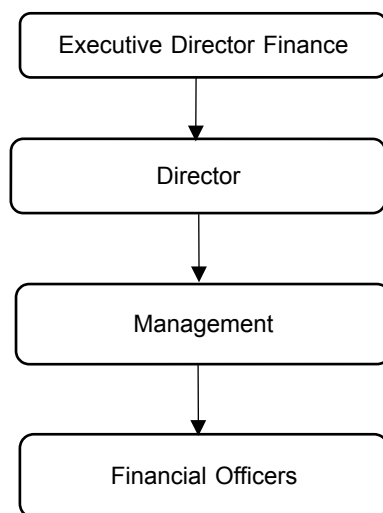


Figure 4.2: Organisational structure Department 2

4.5 Population Identification

Participants from Department 1 were drawn from the Management Support team, which has a subsection named Strategic Support. This subsection is responsible for providing strategic support as well as developing and maintaining comprehensive monitoring, evaluation and information system. The section was primarily chosen because it deals with issues at the centre of this research study and should address the issue of generalizing results. The subsection establishes and maintains a comprehensive information management system. The participants were the Director-General, Deputy Director-General, and junior officers, this cohort of junior officers does secretarial and clerical work for the department. The group interacts with the public a lot. Hence, they are highly vulnerable to cyber-attacks. The participants were all computer literate but not tech-savvy, meaning the groups were highly skilled in end-user computing. For Department 2, only Financial Officers took part in the study. This cohort is vulnerable to security threats, particularly phishing attacks. The group is highly skilled in end-user computing, but like the other group, it is not tech-savvy.

4.6 Research Sample Method

The units of analysis were the individual end-users from both departments. The population aroused great interest because it was a population to which the research hypothesis was applicable. The study adopted a simple random sampling approach, which according to Wellman et al. (2005), ensures that each member of the population has a fair chance of forming part of the sample. Kumar (2011) further notes that in random sampling, participants are not selected on personal preferences, and the selection of one element is totally independent of the selection of the other element(s). A sample of 22 people from Department 1 was drawn from a sample frame of 32. A participation letter inviting participants to participate in the study was used to contact each sample. The letter detailed the experiment's objectives and the entire exercise's duration. Department 2's sample frame was 21, from which a sample of 20 people was drawn. The units of analysis were the users from the two respective departments. Figure 4.3 depicts the process followed by a two-group simple randomized experimental design.

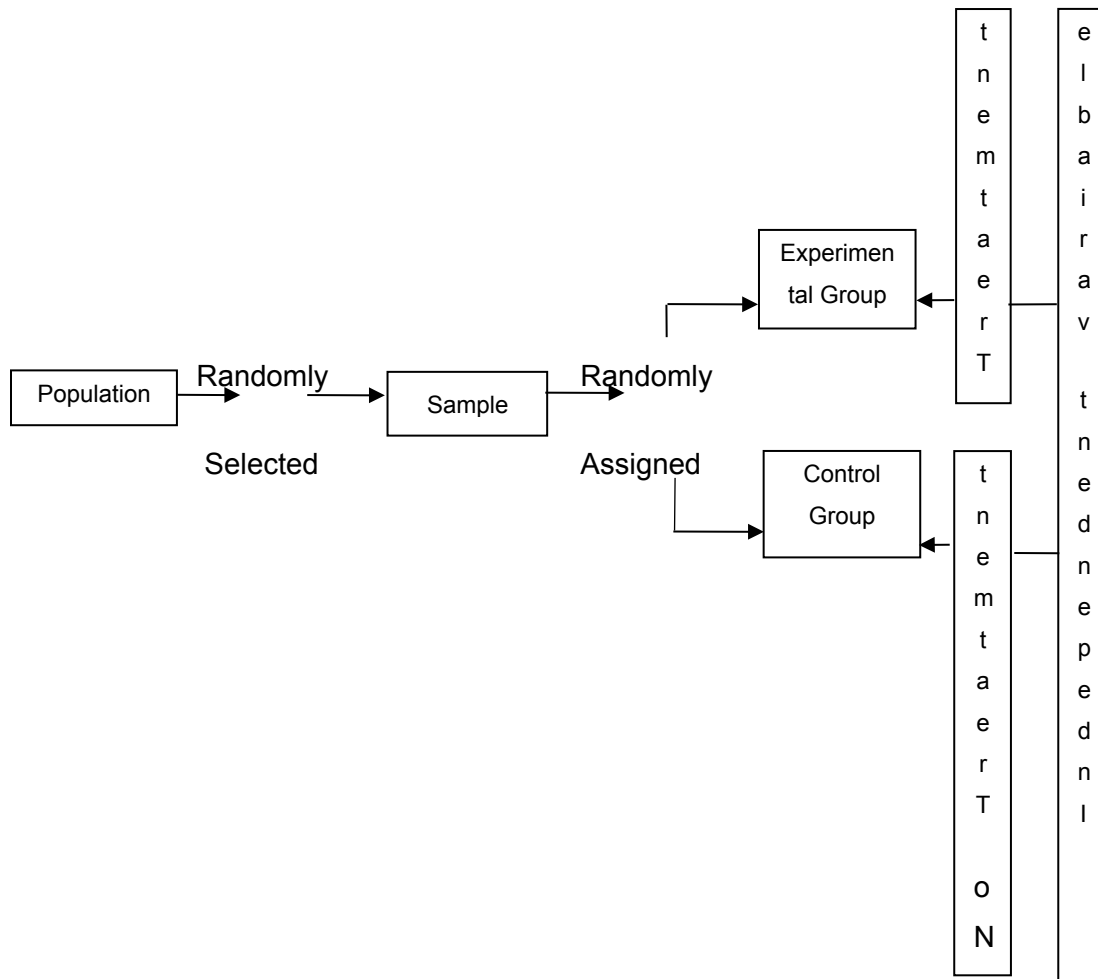


Figure 4.3: Two-group simple randomized experimental design adapted from (Aziz, Subiyanto & Harlanu, 2018)

4.7 Instruments that were used in the experiment

The experiment was conducted at Department 1's virtual centre in Cape Town. The Department provided the venue and the two virtual machines used in the experiment. The two machines were mere terminals connected to a virtual server. The terminals were configured to run Windows 10. The training was conducted on the Microsoft Teams platform. The training focused on Password policy, Phishing and BYOD. Password policy covered the importance of a strong and unique password and the caveats when creating or resetting a password. Phishing focuses on how to identify phishing, smishing and vishing. Phishing uses emails, smishing SMS and vishing voice or phone calls; lastly, phishing covers steps to consider when dealing with phishing. BYOD dealt with the importance of scanning devices for malware programs. Department 2 had their experiment on a virtual platform. The same instruments were used except for the devices. The participants used laptops that ran on Windows 10.

A chatbot was used as a treatment or intervention for the experimental group. The chatbot was designed to provide a message to the experimental group on how to remember the training contents. For instance, a chatbot would remind users about the following essential aspects of creating a strong and unique password for the password policy, identifying a phish and scanning devices.

Bot Message: Your password should always conform to the following password policy requirements: At least eight characters in length, Contains at least 3 of the following four types of characters: lower case letters, upper case letters, numbers, and special characters. For phishing, a chatbot would advise users on the following

Bot Message: 1. Some attachments contain viruses or other malicious programs, so just in general, it is risky to open unknown or unsolicited attachments. 2. Also, in some cases, just clicking on a malicious link can infect a computer, so unless you are sure a link is safe, do not click on it. 3. Email addresses can be faked, so just because the email says it is from someone you know, you cannot be certain of this without checking with the person. 4. Finally, some websites and links look legitimate, but they are hoaxes designed to steal your information. Lastly, for BYOD, a chatbot advised users to remember the following

Bot Message: Scan your portable devices regularly for viruses and other malicious programs. You should have several backup copies stored in separate locations. Encryption is a method to protect against the unauthorized disclosure of information.

Microsoft Excel was used to capture the assessment, record the results of both experimental and control groups, and statistically analyse data. Data collected about the two groups contained the numbers allocated to the users during the random assignment. Users were assigned numbers from 1 – 22. Data about gender and age were also collected.

4.8 Tasks

The tasks performed on the day of the experiment were to conduct training, prepare for the experiment and conduct the experiment. *Conduct training:* training was scheduled for 30 minutes. The training covered three topics: password policy, phishing, and BYOD. Each topic was allocated one-third of the 30 minutes scheduled for training. This means 10 minutes were allocated to discuss the password policy, 10 minutes for phishing and 10 minutes for the BYOD policy. Before the start of the training, users were re-briefed about the ethics, users were reminded that the study would guarantee confidentiality at all costs, participation was voluntary, no rewards for taking part in the study, and participants were free to pull out of the study anytime they felt that their safety or confidentiality was under threat. Lastly, users were informed about the importance of their participation in the study. The purpose of the training was to prepare users for the experiment, ensure participants understood the contents of password policy, phishing, and BYOD policy, and ensure that users were exposed to the same training methods. Participants were all trained simultaneously because, at this stage, they were not assigned to their respective groups.

Prepare for the experiment: preparations for the experiment involved assigning users to their respective groups. This was a two-group design experiment. The groups were experimental and controlled. A random assignment technique was used to allocate participants to the appropriate groups. Participants from Department 1 were assigned numbers from 1 - 22, and participants from Department 2 were assigned numbers from 23 – 42. Participants who were allocated odd numbers were assigned to the control group, and the experimental group participants were given even numbers. Another task during this stage was to ensure that all the tools required to conduct the experiment were working as they should. The tools needed for this experiment were MS Teams, MS Excel, computers and a chatbot.

Conduct the experiment: the purpose of the experiment was explained to both sets of groups. The purpose of the experiment was to test the hypothesis and measure the chatbot's performance. Measuring the chatbot's performance means ascertaining whether the null hypothesis, which states that there is no relation between user compliance and the use of chatbots, should be upheld or disproved. Salkind (2012) argues that the null hypothesis states that the two groups in our research, the experimental and control groups are not different. If this statement is true, the null hypothesis will be accepted; however, if the opposite is true, the null hypothesis will be rejected. Expectations for each group were outlined. Instructions were discussed to ensure participants were fully aware of what was required.

The experiment was conducted in two different settings, the experiment for Department 1 was conducted in a physical setting, and for Department 2, the experiment was conducted on a virtual platform. Participants were given clear instructions; the control group was advised to base their actions or selection of the appropriate action on what was discussed during the training, and for the experimental group, the instructions were that they should make use of the chatbot's messages before selecting the appropriate action because the information contained by a chatbot was meant to help them remember what was discussed during the training. The parameters observed during the experiment were strong passwords, attachments and links, scan devices and encrypted files. The experiment measured how frequently users created a strong password, opened attachments and links, encrypted confidential files or scanned the devices before using them on the company network.

4.9 Procedures

On the day of the experiment, a 30-minute training was conducted via Microsoft Teams. The use of Microsoft Teams was to ensure participants' safety and abide by the COVID-19 protocols. The training material covered: Password policy, BYOD policy and Phishing. The information about the ISPs is freely published by Cyber Security Standards (Appendix B). Users were trained in creating passwords that were compliant with the security policy. Password policy states that:

1. A strong password must be at least eight characters long.
2. It should not contain your personal information, specifically your real name, username, or company name.

3. It must be very unique from your previously used passwords.
4. It should not contain any words spelt completely.
5. It should contain characters from the four primary categories, including uppercase letters, lowercase letters, numbers, and characters.

Phishing material that was covered.

1. Don't trust the display name
2. Look but don't click
3. Check for spelling mistakes
4. Analyse the salutation
5. Don't give up personal or company confidential information
6. Beware of urgent or threatening language in the subject line
7. Don't click on attachments
8. Review the signature
9. Don't trust the header from the email address
10. Don't believe everything you see
11. If not sure, contact the IT security team

BYOD policy.

1. Scan device for viruses and other malicious programs
2. Encrypt to protect information
3. Backup valuable information
4. Check the policy for permitted Apps.

Using a random assignment method, participants were assigned to the control and experimental groups. Participants were assigned numbers from 1 to 22, the odd numbers were assigned to the control group, and the even numbers were assigned to the experimental group. The experiment observed the users' behaviour on the independent variables, strong passwords, attachments and links, and scan devices to establish their influence on the dependent variables, compliance and non-compliance. The assessment was scheduled for 15 minutes per participant, five minutes for Password policy, five minutes for BYOD, and five minutes for Phishing scenarios. Both groups were assessed simultaneously. The only difference between the two groups was the use of chatbots. The experimental group had the opportunity to use a chatbot before taking appropriate security action. For instance, if a user needed to change a password, use an external device, or attend to an urgent email, a chatbot

would proactively guide the user about the three parameters being measured. A chatbot was created on MS Excel for the experimental group. Therefore, there was no installation required. The virtual resource centre could accommodate four participants at a time. However, to ensure the safety of the participants, only two participants were allowed per session.

4.10 Procedural Analysis

Procedural task analysis is a series of tasks necessary to accomplish an objective (Henderson & Feiner, 2011). Figure 4.4 depicts a sequence of tasks required to complete the experiment. The first task involved training users, and then the next task was to prepare the experiment and assign users to their respective groups. The experimental group received an intervention, and no treatment was administered to the control group. The last task was to carry out the actual experiment.

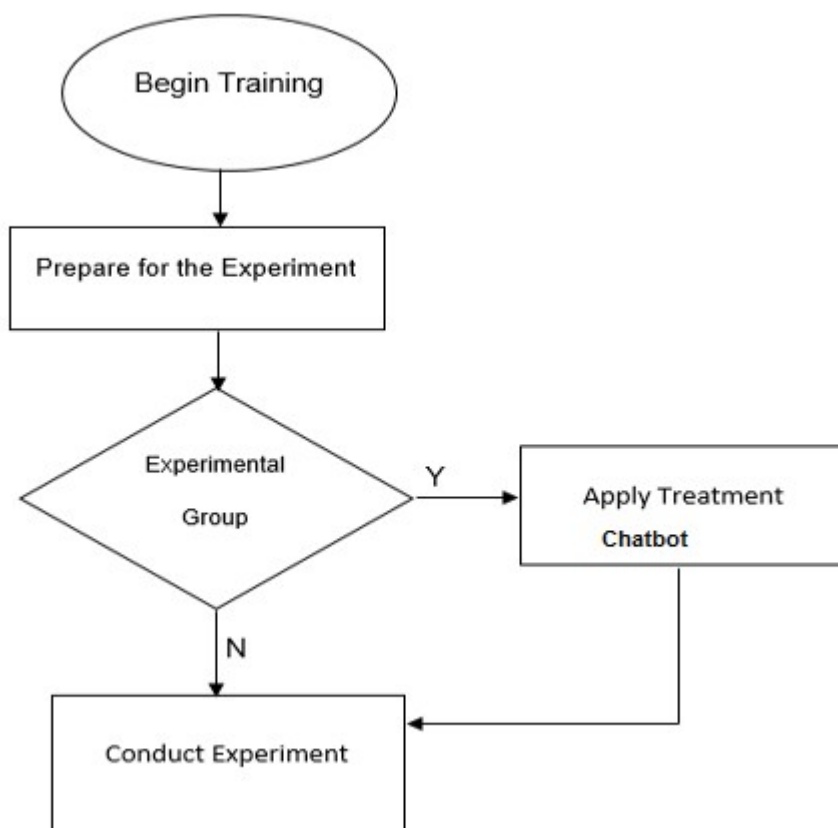


Figure 4.4: Procedural task analysis

4.11 Chatbot Architectural Design

Chatbot design and definition were created by Build a Bot Excel plugins. The version that supports this feature is Microsoft Office 365. The design is the same for both Windows 32-bit version and Windows 64-bit version. This no-code chatbot requires no programming at all and no installation. The benefit of this design is the control over the definitions. There are several ways a bot can be created on Excel; however, the following setup was carried out for this bot. The first step required to run a bot on excel is to create a folder and copy the contents of Build a Bot to your machine. The next step is to open the BotConfig.xlsx spreadsheet and select the bot info tab. Enter the information on the spreadsheet that the bot will run on. The last step is to open another spreadsheet tab that will contain questions that will be answered by a bot or information that a bot will provide to the users.

4.12 Protocol Deviation

The initial plan was to conduct the training session in a physical setting, where all the participants would physically attend the training. A conference room was booked for the training of all the participants. However, due to the COVID-19 pandemic, this arrangement would have harmed the participants, thus compromising the ethics. The second option was to take 2 – 4 participants per training session and organize multiple sessions. This option looked ideal under the circumstances; however, the major issue was time, participants still needed to perform their duties, and therefore, this option had to be ruled out. In light of the above-mentioned minor challenges, deviating from the initial plan was necessary. To ensure participants' safety and that the experiment concluded within the agreed time, the training session was moved to a virtual platform, Microsoft Teams, to be precise.

4.13 Summary

This chapter covered the researcher's process during the experiment and the data gathering. The chapter discussed the goals of the experiment, provided a brief background of the population that was used in the study, discussed the hypothesis and the variables, explained how the population for the study was identified, the sampling method that was used in the study, the instruments that were used to conduct the experiment and procedures that were followed during the experiment. The chapter also discussed the tasks completed during the

experiment, the procedural task analysis, the chatbot's architectural design, and the deviation from the protocol.

CHAPTER FIVE: RESULTS

5.1 Introduction

This study's objective was to ascertain if the use of chatbots could improve the compliance behaviour of users. This chapter starts by providing a descriptive statistical analysis of the scores of the experimental and control groups. Inferential statistics are employed to present the hypothesis's results, i.e., whether we reject or accept the null hypothesis.

5.2 Descriptive statistics

The demographic data of the sample was collected from the two Departments that participated in the research experiment. In Department 1, the number of males who participated in the experiment was 12, and the number of females was 10; for Department 2, the number of males was 18, and there were two females. Tables 5.1 and 5.2 present the frequency of gender for the sampled data. Twenty-two users from Department 1 participated in the experiment. The demographic data for the participants depicted in table 5.1 shows that in the age category between 20 to 29, 0 males and two females participated in the experiment. In the 30 to 39 age category, seven males and one female. The category between 40 to 49 had three males and six females, and for the category 50 to 60, two males and one female took part in the experiment.

Table 5.1: Department 1 Demographics data for the sample

Age	20 - 29	30 - 39	40 - 49	50 - 60
Male	0	7	3	2
Female	2	1	6	1

Table 5.2 depicts the demographic data of Department 2. There were 20 users who participated in this research experiment, nine males and two females in the age category 20 to 29, 8 males and 0 females in the category 30 to 39, 1 male and 0 female in the category 40 to 49, and there were zero participants in the category 50 to 60 years.

Table 5.2: Department 2 Demographics data for the sample.

Age	20 - 29	30 - 39	40 - 49	50 - 60
Male	9	8	1	0
Female	2	0	0	0

Two experiments were conducted for this research study, the first was conducted in Department 1, and in the second, participants were drawn from Department 2. The scores for experiment one are presented below using a scatter chart for Department 1, and for the second experiment, the scores are presented using a bar chart for Department 2. Figure 5.1 and figure 5.2 present the scores of the experimental group and control group for experiment one. Figures 5.3 and 5.4 present the scores for experiment two. The scores for experiment one were as follows: for the experimental group, 11 participants took part in the experiment. The highest score was 7 out of 9, and four participants achieved the highest score. One participant achieved 6 out of 9. Two participants achieved a score of 5 out of 9. Two participants scored 4 out of 9. The lowest score was 3 out of 9, and two participants received a score of 3.

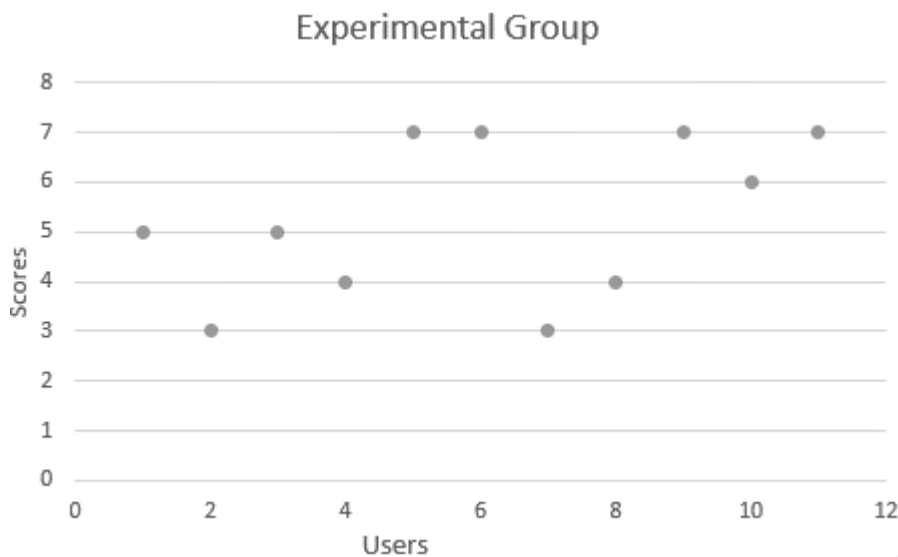


Figure 5.1: Scatter Chart Experimental Group Department 1

The control group had 11 participants. One participant achieved the highest score of 8 out of 9. Three participants scored 7 out of 9. Three participants scored 6 out of 9. One participant scored a 5 out of 9. Four participants scored 5 out of 9. One participant achieved a mark of 3 out of 9. The lowest mark for the control group was 1 out of 9. One participant scored the lowest mark of 1 out of 9.

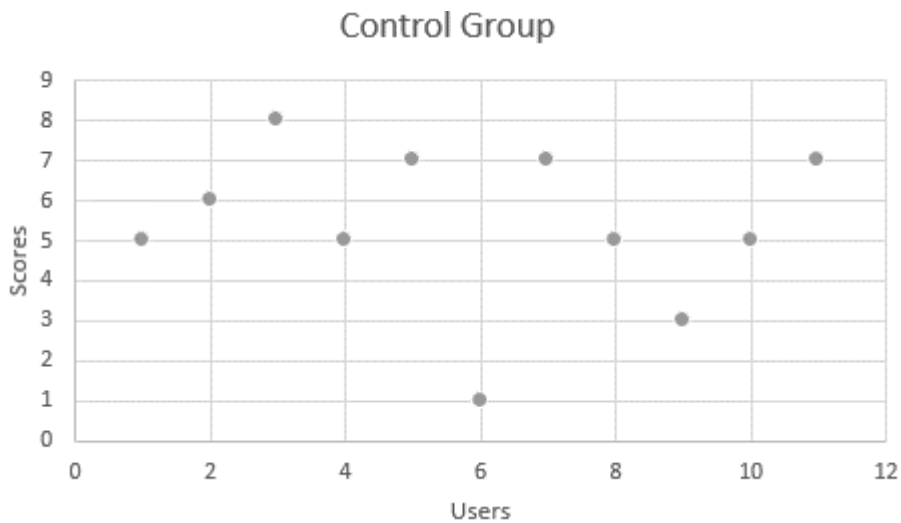


Figure 5.2: Scatter Chart Control Group Department 1

The results for experiment two were as follows: for the experimental group, ten users took part in the study. Three users scored the highest score of 7 out of 9. One user achieved a 6 out of 9. Four users obtained a score of 5 out of 9. One user scored a 4 out of 9. The lowest score was 3 out of 9, of which only one user obtained this score.

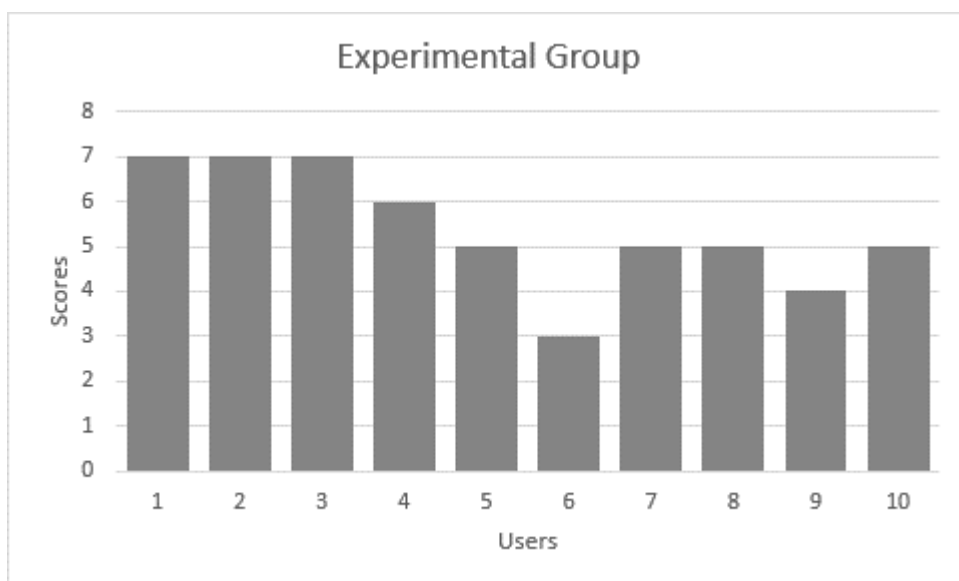


Figure 5.3: Bar Chart Experimental Group Department 2

The control group scores for experiment two, where ten users participated in the study. One user scored the highest score of 4 out of 9. One user scored a 3 out of 9. Six users obtained a 1 out of 9. Two users scored the lowest score of zero out of 9.

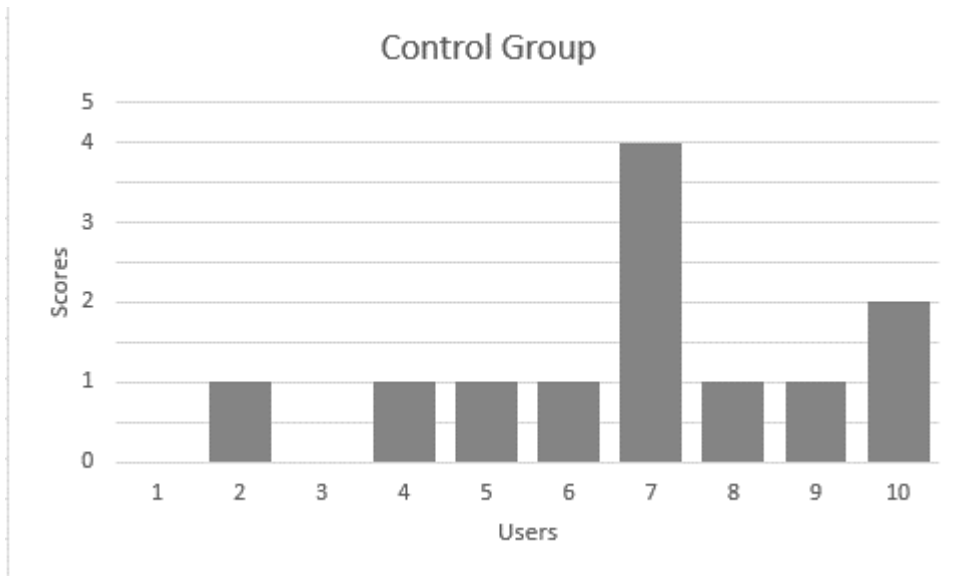


Figure 5.4: Bar Chart Control Group Department 2

Measures of central tendency and dispersion experiment one: the experimental group had a sum of 58, a mean score of 5,27, a median of 5, a mode of 7, a standard deviation of 1,62, a range of 4, a minimum score of 3, and a maximum score of 7. Data skewness was slightly negative.

Table 5.3: Measures of central tendency and dispersion Experimental group

Mean	5,27
Standard Error	0,49
Median	5
Mode	7
Standard Deviation	1,62
Sample Variance	2,62
Kurtosis	-1,64
Skewness	-0,19
Range	4
Minimum	3
Maximum	7
Sum	58
Count	11
Confidence Level	(95,0%)

The control group had a sum of 59, a mean score of 5.36, a median of 5, a mode of 5, a standard deviation of 2,01, a range of 7, a minimum score of 1, and a maximum score of 8. The data skewness was more to the left.

Table 5.4: Measures of central tendency and dispersion Control group

Mean	5,36
Standard Error	0,61
Median	5
Mode	5
Standard Deviation	2,01
Sample Variance	4,05
Kurtosis	1,01
Skewness	-0,97
Range	7
Minimum	1
Maximum	8
Sum	59
Count	11
Confidence Level	(95,0%)

Measures of central tendency and dispersion experiment two: The sum of the experimental group was 54, and the count was 10. The mean score for the experimental group was 5,4, with a median of 5 and a mode of 5. The minimum was 3, the maximum was seven, and the range was 4. The data set's standard deviation was 1.35, and the data was negatively skewed.

Table 5.5: Measures of central tendency and dispersion experimental group

Mean	5,4
Standard Error	0,43
Median	5
Mode	5
Standard Deviation	1,35
Sample Variance	1,82
Kurtosis	-0,6
Skewness	-0,24
Range	4
Minimum	3
Maximum	7
Sum	54
Count	10
Confidence Level	95,00%

The total score or sum of the control group was 12. The count was 10. The data set's mean was 1.2, the median was 1, and the mode was 1. The minimum score for the control group was 0, the maximum score was four, and the range was 4. The data set's standard deviation was 1.14, and the skewness was more to the right.

Table 5.6: Measures of central tendency and dispersion control group

Mean	1,2
Standard Error	0,36
Median	1
Mode	1
Standard Deviation	1,14
Sample Variance	1,29
Kurtosis	4,34
Skewness	1,8
Range	4
Minimum	0
Maximum	4
Sum	12
Count	10
Confidence Level	95,00%

5.3 Hypothesis Testing

The research hypothesis focused on the differences between users who were exposed to a chatbot as a treatment and users who did not receive treatment. The null and alternative hypotheses were:

H_0 : There is no relation between user compliance and the use of chatbots.

H_1 : There is a positive relationship between improved user password compliance behaviour and the use of chatbots. H_1 , Department 1, the mean average for the control group was 2.18, and the standard deviation was 0,72. The mean average for the experimental group was 2.27, and the standard deviation was 0,75. Figure 5.5 shows the control and experimental groups' mean averages and standard deviations, respectively.

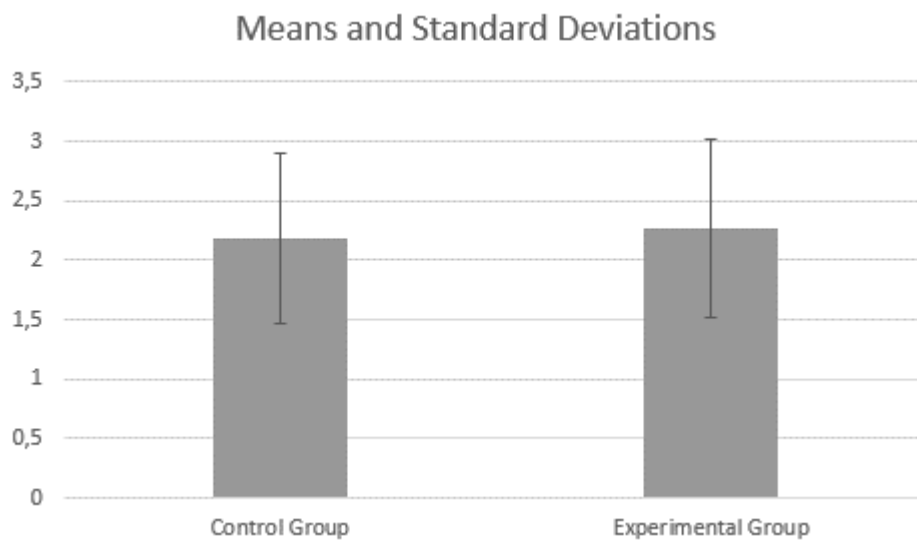


Figure 5.5: H₁ Means and Standard Deviations Department 1

H₁ Department 2, the mean average for the control group was 0,4, and the standard deviation was 0,49, whereas for the experimental group, the mean average was 1,7, and the standard deviation was 0,46. Figure 5.6 shows the control and experimental groups' mean averages and standard deviations.

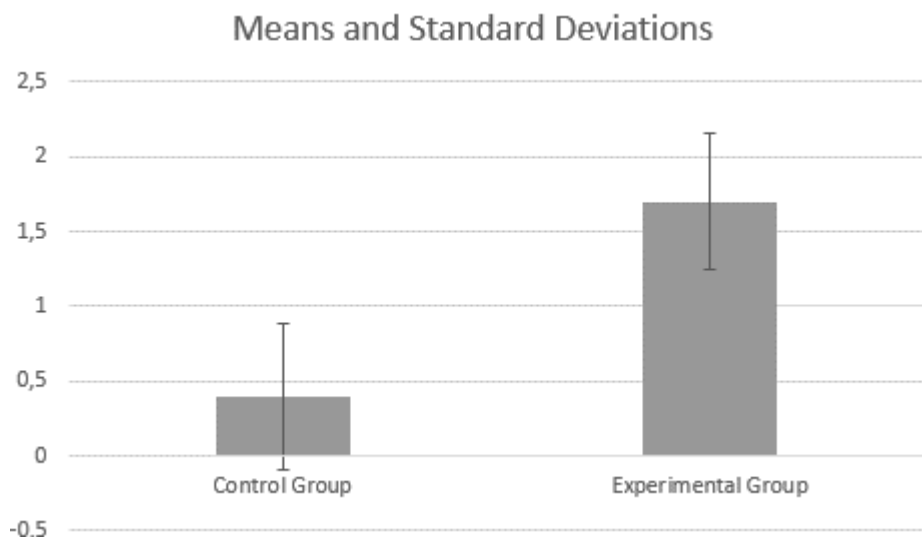


Figure 5.6: H₁ Means and Standard Deviations Department 2

H₂: There is a strong relationship between users' ability to spot a phish and the use of chatbot
H₂ Department 1, the mean and standard deviation results were mean averages for the control group 1,45 and the standard deviation 0,99. The experimental group's mean average was 1,18,

and the standard deviation was 0,72. Figure 5.7 depicts the mean averages and standard deviations of hypothesis 2 for Department 1.

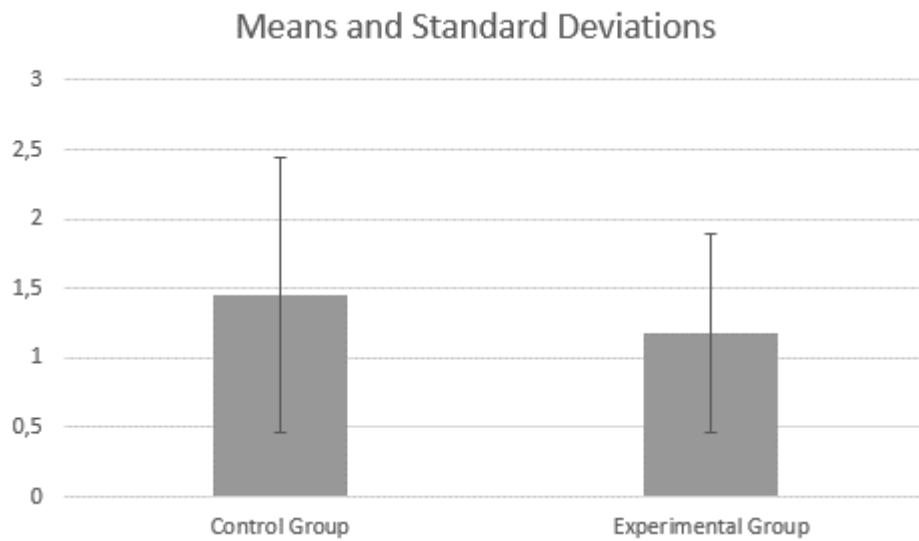


Figure 5.7: H₂ Means and Standard Deviations Department 1

H₂ Department 2, the mean average for the control group was 0,4, and the standard deviation was 0,49. For the experimental group, the average mean was 0,9, and the standard deviation was 0,83. Figure 5.8 depicts the mean averages and standard deviations of hypothesis 2 for Department 2.

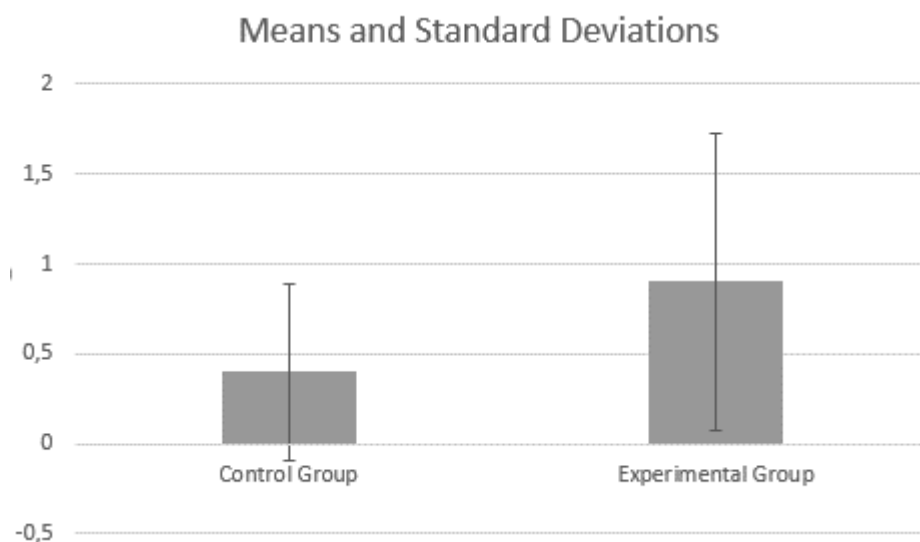


Figure 5.8: H₂ Means and Standard Deviations Department 2

H₃: There is a positive relationship between users who scan their portable devices before using them on the company network and chatbot use. H₃ Department 1 had a mean average of 1,73 and a standard deviation of 0,86 for the control group. The experimental group had a mean average of 1,91 and a standard deviation of 0,90. Figure 5.9 illustrates the control and experimental groups' mean averages and standard deviations, respectively.

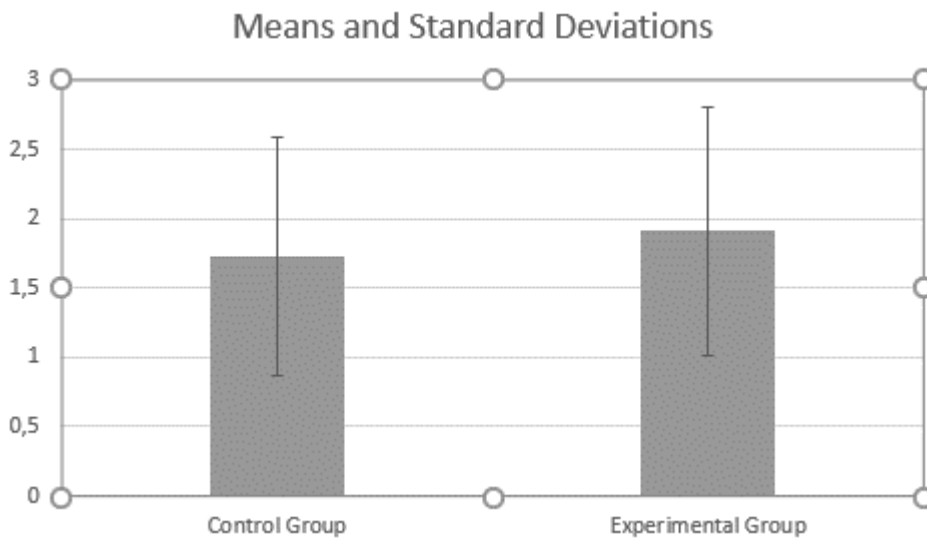


Figure 5.9: H₃ Means and Standard Deviations Department 1

H₃ Department 2, the control group, had an average mean of 0.3 and a standard deviation of 0,46. The experimental group mean was 2,7, and the standard deviation was 0,49. Figure 5.10 illustrates the control and experimental groups' mean averages and standard deviations, respectively.

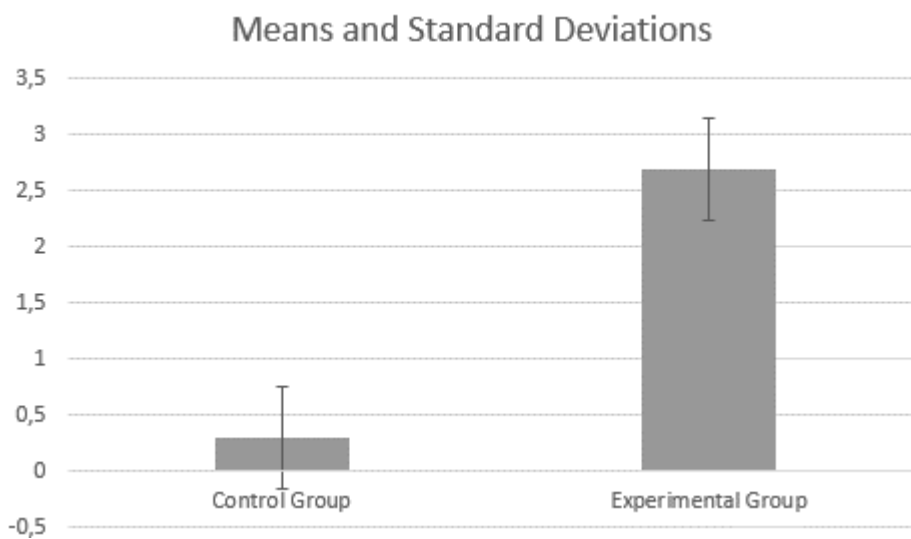


Figure 5.10: H₃ Means and Standard Deviations Department 2

The hypothesis test was done at a 5% significance level, i.e., $P = 0.05$. A t-test described in chapter 1, section 1.11, was used to test whether there was a statistical difference between the means of the two groups. The t-test used two independent samples and a one-tailed test.

H₁ Results Department 1

Eleven participants from the experimental group received treatment ($M = 2.27$, $SD = 0,75$) compared to the 11 participants in the control group ($M = 2,18$, $SD = 0,72$). The results showed statistical significance. The t-test suggested that the results were statistically significant $t(20) = 12,07$, $p = 0.001$. The results proved significant at $p < 0.05$; therefore, we can reject the null hypothesis.

H₁ Results Department 2

The intervention was administered to 10 participants from the experimental group ($M = 1,7$, $SD = 0,46$). The control group also had 10 participants ($M = 0,4$, $SD = 0,49$). The results showed statistical significance. The 10 participants who were exposed to the treatment ($M = 1,7$, $SD = 0,46$) compared to the 10 participants who did not receive the intervention ($M = 0,4$, $SD = 0,46$) showed significantly better levels of compliance, $t(18) = -193,79$, $p = 0.001$. Thus, we can refute the null hypothesis.

H₂ Results Department 1

Eleven participants from the experimental group who treatment ($M = 1,18$, $SD = 0,72$) compared to the 11 participants in the control group ($M = 1,45$, $SD = 0,99$). The results showed no statistical significance. The t-test suggests that the results are not statistically significant $t(20) = -0.61$ $p = 0.28$, two independent samples and a one-tailed test. The results proved insignificant at $p < 0.05$; therefore, we cannot reject the null hypothesis.

H₂ Results Department 2

The treatment was administered to 10 participants from the experimental group ($M = 0,9$, $SD = 0,83$). The control group also had 10 participants ($M = 0,4$, $SD = 0,49$). The results showed statistical significance. The 10 participants who were exposed to the treatment ($M = 0,9$, $SD = 0,83$) compared to the 10 participants who did not receive the intervention ($M = 0,4$, $SD = 0,49$)

showed significantly better levels of compliance, $t(18) = 6.58$, $p = 0.001$. Accordingly, we can reject the null hypothesis.

H₃ Results Department 1

Eleven participants from the experimental group received treatment ($M = 1,91$, $SD = 0,90$) compared to the 11 participants in the control group ($M = 1,73$, $SD = 0,86$). The results showed statistical significance. The t-test proved that the results were statistically significant $t(20) = 21.11$ $p = 0.001$. The results proved significant at $p < 0.05$; therefore, we can reject the null hypothesis.

H₃ Results Department 2

The intervention was administered to 10 participants from the experimental group ($M = 2,7$, $SD = 0,46$). The control group also had 10 participants ($M = 0,3$, $SD = 0,46$). The 10 participants who were exposed to the treatment ($M = 2,7$, $SD = 0,46$) compared to the 10 participants who did not receive the intervention ($M = 0,4$, $SD = 0,49$) showed significantly better levels of compliance, $t(18) = -342.86$, $p = 0.001$. Consequently, we can reject the null hypothesis.

5.4 Summary

This chapter provided a statistical account of the results obtained from the two experiments conducted to test the hypothesis. The introduction gave a brief discussion of the objectives of the study. Descriptive statistics methods to compare the results of the two groups were then used to provide a detailed analysis of the results. Lastly, a hypothesis test or p-test to ascertain whether to reject the null hypothesis or not was conducted using a t-test method.

CHAPTER SIX: DISCUSSIONS AND IMPLICATIONS

6.1 Introduction

This chapter concludes the study by recapping the aims and research objectives. The chapter also discusses the results, future research and recommendations, implications and limitations. Lastly, the chapter finishes with a discussion about what the study accomplished. The study aimed to determine the impact of a chatbot in enforcing ongoing user compliance in selected government entities. This was achieved by testing three hypotheses. Table 6.1 depicts the research objectives and hypotheses.

Table 6.1: Objectives and Hypotheses.

Objectives	Hypothesis
Conduct the experiment using a chatbot as a treatment, and	H₁ : There is a positive relationship between improved user password compliance behaviour and the use of chatbots
Ascertain whether the use of chatbots can improve ISP compliance	H₂ : There is a strong relationship between users' ability to spot a phish and the use of chatbot H₃ : There is a positive relationship between users who scan their portable devices before using them on the company network and the use of chatbots

6.2 Discussion of results

The results for the first hypothesis indicated a significant difference at $p = 0.001$ for both departments. Thus, the study could reject the null hypothesis. The results for the second hypothesis were insignificantly different at $p = 0.28$ for Department 1. Consequently, we failed to reject the null hypothesis. The results of the third hypothesis proved significantly different at 0.001 , so we could refute the null hypothesis. This means the results did not support the current literature for the first hypothesis, and the null hypothesis could not be upheld. The results mean that users' password compliance can be improved if users constantly receive a reminder about the contents of the password policy.

In the second hypothesis, the results of the first experiment 1 supported the current literature and could not reject the null hypothesis. The results of the second experiment proved statistically significant. Considering the contrasting results, this means there is no evidence that a dedicated information security training method would help users manage phishing attacks effectively. The results mean that users' compliance is quite convoluted and cannot be pinned on one aspect of ISP and, in this case, training methods (Puhakainen & Siponen, 2015). Karlsson, Kolkowska and Hedstro (2013) add that compliance depends on the user's desire to follow training and awareness methods. The success of ISP necessitates users' endorsement, and users need to commit to compliance and see the need to maintain compliant behaviour. ISP compliance is simply an issue of human conduct (Ali et al., 2021).

In the third hypothesis, the test results of Departments 1 and 2 supported the hypothesis. The results showed a significant difference between users who received a constant reminder about the contents of the BYOD policy and those who did not receive any form of reminder. The results are in accordance with the supposition that using chatbots can improve BYOD compliance behaviour. The discrepancy in the results could be ascribed to different settings in which the experiments were conducted. Figure 2.3 highlights the effect of factors based on the Theory of Planned Behaviour. The theory listed environmental factors among the major influences on users' behaviour. The first experiment was conducted in a physical setting, whereas the second was in a virtual setting. Sommer (2011) argues that habitual behaviour is possible due to regular behaviour in familiar settings. Greaves, Zibarras and Stride (2013) add that environmental factors influence user behaviour.

Another behavioural model that can explain the reason behind the disparity in the results is the Johari window model discussed in chapter two. This method implies that users' security conduct can be explained using the security grid, i.e., open, blind, unknown, and hidden. The results failed to uphold the hypothesis though users received security training and were exposed to a chatbot. Therefore, the quadrants unknown and hidden would indicate how participants conducted themselves during the experiment.

6.3 Implications

The results of the first hypothesis proved statistically significant and thus upheld the hypothesis. The second hypothesis results failed to reject the null hypothesis. This means the treatment did not affect the security conduct of the participants. These findings are, therefore, in line with the extant literature. However, the results of the third hypothesis showed a clear correlation between users' BYOD policy compliance and chatbot use in relation to the study's objectives. The results show that organisations can advance end-user compliance using chatbots. A mechanism that can constantly remind users about ISP contents can enforce end-user compliance. Compliance levels can improve with regular exposure to the contents of ISP.

6.4 Limitations

Limitations of the research methodology were discussed extensively in chapter three. Issues about educational significance, failure to explain cause-effect relationships, generalizability, time, cost and the objective nature of the study were all listed among the major limitations of quantitative research. One of the major limitations of this study was generalizability. The study failed to draw a larger sample that could have justified generalizability to a broader population. For this reason, the results could not be generalized to all government entities. However, the study's sample size was large enough to ensure that results could be generalized to the two departments participating in the study. In other words, the generalizability of the results will be limited to the populations of Department 1 and Department 2.

6.5 What the study accomplished

The study proved that chatbots could be used in the information security domain. It highlighted that ISP training should be conducted periodically, yet users are expected to worry about their daily operations and the contents of ISP. Furthermore, the study has identified a lack of a mechanism that can aid users in remaining compliant at all times. This study has proved that chatbots can constantly remind users about the contents of ISP. Consequently, that can improve users' compliance levels and eliminate the perception that compliance is an arduous task that needs to be performed periodically. The study also showed that chatbots could be incorporated with the current training delivery methods to ensure that users receive after-training support. This will, of course, improve the retention of ISP contents, which means users will receive constant reminders about the contents of the ISP. Lastly, the study has laid a solid

foundation for future research. The study pointed out that there is a gap in the current literature when it comes to ensuring ongoing ISP compliance. The study also noted a lack of research on enforcing ongoing IS compliance using chatbots.

6.6 Future Research and Recommendations

Follow-up research can improve the study with unlimited time and budget. Therefore, it is recommended that this study benefits from a longitudinal research study, in which all participants can be observed over an extended period. The research can be improved by extending the study to other provinces. Future research can further analyse the delivery methods and assess their efficacy in delivering information security training. The steps required to implement these recommendations can be found in chapter four, the experiment process.

6.7 Summary

This chapter concluded the study and revisited the aim and objectives. The chapter also discussed the results obtained during the experiment and their significance in the existing theory and knowledge.

References

- Abdelsadeq, Z.A., Omar, S.N., Basir, N. and Rafei, N.F.N.B.M. 2019. Unintentional Insider Threats Countermeasures Model (UITCM). In *2019 International Conference on Cybersecurity (ICoCSec)*, 53-58.
- Abdul-kader, S. A. 2015. Survey on Chatbot Design Techniques in Speech Conversation Systems. *International Journal of Advanced Computer Science and Applications*, 6(7): 72–80.
- Abraham, S. and Nair, S. 2014. Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains. *Journal of Communications*, 9: 899-907.
- Adamopoulou, E. and Moussiades, L. 2020. An Overview of Chatbot Technology. *International Federation for Information Processing 2020*: 373–383.
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M. and Wang, Y. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3): 1-41.
- Adam, M., Wessel, M. and Benlian, A., 2021. AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets*, 31(2): 427-445.
- 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): 438–441.
- Aguboshim, F. C. and Udobi, J. I. 2019. Security Issues with Mobile IT : A Narrative Review of Bring Your Own Device (BYOD). *Journal of Information Engineering and Applications*, 9(1): 56–66.
- Ahmaad, Z., Norhashim, M., Song, O.T. and Hui, L.T. 2016. A typology of employees' information security behaviour. In *2016 4th International Conference on Informational Communication Technology*, 1-4.
- Akhtar, I. 2016. *Research in Social Science: Interdisciplinary Perspectives*. 1st Edition. Kanpur: Social research foundation. 17 – 25.
- Alabdan, R. 2020. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 2-5.

Aldawood, H. and Skinner, G. 2018. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68.

Aldawood, H. & Skinner, G. 2020. An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, 177(30): 1-11.

Al-Darwish, A.I. and Choe, P. 2019. A framework of information security integrated with human factors. In *International Conference on Human-Computer Interaction*: 217-229. Springer, Cham.

Alfawaz, S., Nelson, K. and Mohannak, K. 2010. Information security culture: a behaviour compliance conceptual framework. *AISC*, 105: 1–11.

Algarni, M., Almesalm, S. and Syed, M. 2018. Towards enhanced comprehension of human errors in cybersecurity attacks. In *International Conference on Applied Human Factors and Ergonomics*, 163-175.

Alghamdi, S., Win, K. and Vlahu-Gjorgievska, E. 2020. Information Security Governance Challenges and Critical Success Factors: Systematic Review. *Computer & Security*, 4-10.

Alhassan, M. M. and Adjei-Quaye, A. 2017. Information Security in an Organization. *International Journal of Computer*, 9–18.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M. and Sohail, A. 2021. Information Security Behaviour and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, 1 - 5, April.

Alkalbani, A., Deng, H. and Kam, B. 2014. A Conceptual Framework for Information Security in Public Organizations for E-Government Development. *Australasian Conference on Information Systems*, 1–11 December.

Alkalbani, A., Deng, H. and Zhang, X. J. 2016. Investigating the Impact of Institutional Pressures on Information Security Compliance in Organizations 2 Literature Review. *Australasian Conference on Information Systems*, 1–12.

Alkalbani, A., Deng, H. and Kam, B. 2018. Organizational Security Culture and Information Security Compliance For E-Government Development: The Moderating Effect Of Social. *Australasian Conference on Information Systems*, 1–11.

- Al-Omari, A., El-Gayar, O. and Deokar, A. 2012. Information security policy compliance: The role of information security awareness. *Proceedings of the Eighteenth Americas Conference on Information Systems*, Seattle, 9-12 August 2012, 1633–1640
- Al-omari, A., Deokar, A., El-gayar, O., Walters, J. and Yarmouk, H. A. 2013. Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *46th Hawaii International Conference on System Sciences 2013*, 1-10.
- Alotaibi, M., Furnell, S. and Clarke, N. 2016. A novel model for monitoring security policy compliance. *Journal of Internet Technology and Secured Transactions*, 5(3): 4-6.
- Alotaibi, M., Furnell, S. and Clarke, N. 2017. Information security policies: A review of challenges & influencing factors. *11th International Conference for Internet Technology and Secured Transactions 2016*, 352–358.
- Alotaibi, M. J. 2017. A model for monitoring end-user security policy compliance. Unpublished PhD thesis, Plymouth University, Plymouth. 24-40.
- Alotaibi, M. 2019. A Framework for Reporting and Dealing with End-User Security Policy Compliance. *Information and Computer Security*: 3–23.
- Al Salek, A. 2021. Information Security Awareness Training for End-User: A Survey on The Perspective of Nordic Municipalities. Unpublished Bachelor Thesis, University of Skövde, Skövde. 6-10.
- Al-Shanfari, I., Yassin, W. and Abdullah, R. 2020. Identify of factors affecting information security awareness and weight analysis Process. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(3): 534-42.
- Alyami, A., Sammon, D., Neville, K. and Mahony, C. 2020. Exploring IS security themes: a literature analysis. *Journal of Decision Systems*, 29: 425-437.
- Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. and Choudrie, J. 2021. Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, 114:106531.
- Anderson, D., Abiodun, O.P. and Christoffels, A. 2020. Information Security at South African Universities: Implications for Biomedical Research. *International Data Privacy Law*, 10(2): 180-186.

- Andre, E. and Pelachaud, C. 2016. Interacting with Embodied Conversational Agents. *Multimedia Concepts and Applications*: 5-8.
- Andronova, I., Belova, I. N., Ganeeva, M. V. and Moseykin, Y. N. 2018. Scientific technical cooperation within the EAEU as a key factor of the loyalty of the participating countries, population to the integration and of its attractiveness for new members. *RUDN Journal of Sociology*, 18(1): 117–130.
- Angst, C.M., Block, E.S., D'arcy, J. and Kelley, K., 2017. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches*, 893-916.
- Antwi, S. K. and Hamza K. 2015. Qualitative and Quantitative Research Paradigms in Business Research: A Philosophical Reflection. *European Journal of Business and Management*, 7(3): 217 – 230.
- Apuke, O. 2017. Quantitative Research Methods: A Synopsis Approach. *Arabian Journal of Business and Management Review*: 40-47.
- Asenahabi, B., M. 2019. Basics of Research Design: A Guide to selecting appropriate research design. *International Journal of Contemporary Applied Research*, 6(5): 77 - 80.
- Augello, A., Pilato, G., Machi, A. and Gaglio, S. 2012. An Approach to Enhance Chatbot Semantic Power and Maintainability: Experiences within the FRASI Project. *2012 IEEE Sixth International Conference on Semantic Computing 2012*, 2–8
- Aziz, A. N., Subiyanto, S. and Harlanu, M. 2018. Effects of the Digital Game-Based Learning on Students Academic Performance in Arabic Learning at Sambas Purbalingga. *Journal of Social and Islamic Culture*, 26(1): 1-2.
- Azmi, R., Tibben, W. and Win, K.T. 2018. Review of cybersecurity frameworks: context and shared concepts. *Journal of cyber policy*, 3(2): 258-283.
- Babar, Z., Lapouchnian, A. and Yu, E. 2011. Chatbot Design - Reasoning about design options using i * and process architecture Analysing Social Implications of Process Architecture Reconfigurations. *iStar*: 2-6.

Bada, M., Sasse, A. M. and Nurse, J. R. C. 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 2-9.

Bada, M. and Nurse, J.R. 2019. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*: 7-9.

Baker, C. 2019. *Foundations*. 1st Edition. Jones & Bartlett Learning: Burlington. 157 – 180.

Balozian, P. and Leidner, D. 2017. Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *The Database for Advances in Information Systems*, 48(3): 11–43.

Balozian, P., Leidner, D. and Warkentin, M. 2019. Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 59(3): 197-210.

Banfield, J. M. 2016. A study of information security awareness program effectiveness in predicting end-user security behaviour. Unpublished PhD thesis, Eastern Michigan University, Michigan. 13–50.

Bann, L. L., Singh, M. M. and Samsudin, A. (2015). Trusted security policies for tackling advanced persistent threats via spear phishing in BYOD environment. *Procedia Computer Science*, 72: 129-136.

Barricelli, B. R., Valtolina, S., Di Gaetano, S. and Diliberto, P. 2018. Chatbots and Conversational Interfaces: Three Domains of Use. *Proceedings of the Fifth International Workshop on Cultures of Participation in the Digital Age*, 29 May, 10-25.

Bartsch, S. and Sasse, M., A. 2012. How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization. *International Computer Music Conference*, London, 2-5.

Bauer, S., Bernroider, E. and Chudzikowski, K. 2013. End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study. [AIS SIGSEC Workshop on Information Security & Privacy 2012](#), Milan, 14 June 2020, 11-19.

Bauer, S. and Bernroider, E.W. 2017. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking

- organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 48(3): 44-68.
- Berge, S. H. 2018. Rise Of The Chatbots. Unpublished Masters Thesis, University of Oslo, Oslo. 13-20.
- Baharin, S.H., Asma'Mokhtar, U., Sulaiman, R. and Yusof, M.M. 2019. Issues and trends in information security policy compliance. In *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1-6.
- Bhatia, S., Behal, S. and Ahmed, I. 2018. Distributed denial of service attacks and defense mechanisms: current landscape and future directions. In *Versatile Cybersecurity*: 55-97.
- Bhattacharjee, A. 2012. *Social Science Research: Principles, Methods, and Practices*. 2nd Edi. Florida: Global Text Project. 44-100.
- Behera, B. 2016. Chappie - A Semi-automatic Intelligent Chatbot. *CSE*: 1-5.
- Bhawna, G. and Gobind, E. 2015. Research Methodology and Approaches. *IOSR Journal of Research & Method in Education*, 5(3): 7 – 12.
- Blackwood-brown, C. G. 2018. An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills. Unpublished PhD dissertation, Nova Southeastern University, Florida. 16-30.
- Beris, O., Beautement, A. and Sasse, M. A. 2011. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviours. *Proceedings of the New Security Paradigms Workshop*, 1-12.
- Blaxter, L., Hughes, C. and Tight, M. 2012. *How to Research*. 3rd Edition. Berkshire: Open University Press. 55-80.
- Blum, D. 2020. *Rational Cybersecurity for Business*. Silver Spring: Apress Open. 15-20.
- Blythe, J. M., Coventry, L. and Little, L. 2015. Unpacking security policy compliance: The motivators and barriers of employees. *2015 Symposium on Usable Privacy and Security security behaviours*, 103-122.

- Bogataj, D., Aver, B. and Bogataj, M. 2016. Supply chain risk at simultaneous robust perturbations. *International journal of production economics*, 181: 68-78.
- Boss, S. R., Galletta, D., Lowry, P. B. and Moody, G. D. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly*, 39(4): 837–864, December.
- Brandtzaeg, P.B. and Følstad, A. 2017. Why people use chatbots. In *International conference on internet science*, 377-392.
- Bulgurcu, B., Kajtazi, M., Cavusoglu, H. and Benbasat, I. 2014. Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations. *Proceeds of the 2014 47th Hawaii International Conference on System Sciences*, January, 523–548.
- Burney, S.M.A and Saleem, H. 2008. Inductive & Deductive Research Approach. *IJSER*: 6 – 7.
- Cahn, B. J. 2017. CHATBOT: Architecture, Design, & Development. Senior thesis, University of Pennsylvania, Philadelphia. 3–46.
- Caldarini, G., Jaf, S. and McGarry, K. 2022. A literature survey of recent advances in chatbots. *Information*, 13(1):41.
- Camburn, E.M., Goldring, E., Sebastian, J., May, H. and Huff, J. 2016. An examination of the benefits, limitations, and challenges of conducting randomized experiments with principals. *Educational Administration Quarterly*, 52(2): 187-220.
- Candello, H., Pichiliani, M., Pinhanez, C. and Cavalin, P. 2019. Teaching Chatbots to Show Science: A Study with Museum Guides. *Association for Computing Machinery*: 2–6.
- Chan, K.F.P. and De Souza, P. 2017. Transforming network simulation data to semantic data for network attack planning. In *ICMLG 2017 5th International Conference on Management Leadership and Governance*. Academic Conferences and Publishing Limited, 74
- Chang, S. E. and Lin, C. 2015. Exploring organizational culture for information security management. *Industrial Management & Data Systems*: 20-30.
- Charlette, D. 2015. Cybersecurity Policy Compliance: An Empirical Study of Jamaican Government Agencies. *Proceedings of SIG GlobDev 2015 Pre-ECIS Workshop*, Munster, 26 May 2015, 2–21.

- Chaudhury, S. and Banerjee, A. 2009. Hypothesis testing, type I and type II errors. *Industrial Psychiatry Journal*: 1-6.
- Chaves, A.P. and Gerosa, M.A. 2021. How should my chatbot interact? A survey on social characteristics in human chatbot interaction design. *International Journal of Human-Computer Interaction*, 37(8): 729-758.
- Cheng, L., Li, Y., Li, W., Holm, E. and Zhai Q. 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*: 1–13.
- 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: 74361-74382.
- Ciayandi, A., Mawardi, V.C. and Hendryli, J. 2020. Retrieval Based Chatbot on Tarumanagara University with Multilayer Perceptron. In *IOP Conference Series: Materials Science and Engineering*, 1007(1), 12146.
- Clary, P. C. 2014. You Never Know Who's Watching: How Technology is Shaping Practice for Social Service Professionals. Unpublished PhD dissertation, Kansas State University, Manhattan. 19-72.
- Cohen, R., Mathiarasu, N., Aarif, R., Ansari, S., Fraser, D., Hegde, M., Henderson, J., Kajic, I., Khan, A., Liao, Z., Mancisidor, A., Nagpal, S., Pham, A., Saini, A., Shen, J., Singh, H., Tavares, C. and Thandra, S. 2017 An education-based approach to aid in the prevention of cyberbullying. *ACM Computers & Society* 47(4): 17–28.
- Conteh, N.Y. and Schmick, P.J. 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23): 31.
- Coperich, K., Cudney, E. and Nembhard, H. 2017. Continuous Improvement Study of Chatbot Technologies using a Human Factors Methodology. *Proceedings of the 2017 Industrial and Systems Engineering Conference, 2017*, 1–6.
- Cosima, Rughinis and Razvan, R. 2014. Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *Computers & Security*, 43: 3-10.

- Cram, W.A., Proudfoot, J.G. and D'arcy, J. 2017. Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 26(6): 605-641.
- Crossland, G. and Ertan, A. 2018. Everyday Security in Organizations: A Literature Review. *Conference: Academic Centres of Excellence in Cyber Security*, 12-16.
- Cunningham-Nelson, S., Boles, W., Trouton, L. and Margeri, E. 2019. A Review of Chatbots in Education: Practical Steps Forward. *Proceedings of the AAEE 2019 Conference*, Brisbane, 1 January. 2-8.
- Curran, T.T., 2018. Standardizing instructional definition and content supporting information security compliance requirements. Unpublished PhD dissertation, Nova Southeastern University, Florida. 56-66.
- Dahiya, M. 2017. A Tool of Conversation: Chatbot. *International Journal of Computer Sciences and Engineering*, 5(5): 158–161, May 30.
- Dale, R. 2016. The return of the chatbots. *Natural Language Engineering*, 22(5): 811–817.
- Dang-Pham, D., Pittayachawan, S. and Bruno, V. 2017. Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67: 196-206.
- Das, S., Kim, T., Dabbish, L. A. and Hong, J. I. 2014. The Effect of Social Influence on Security Sensitivity. *Tenth Symposium on Usable Privacy and Security*, California, 11 July 2014, 143–157.
- Datta, S. 2018. Sampling methods. West Bengal University of Animal and Fishery Sciences: 1 – 6.
- Da Veiga, A. and Martins, N. 2017. Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70:72-94.
- Dimitrios, T. and Fountouki, A. 2019. Limitations And Delimitations In The Research Process. *Perioperative nursing*, 7(3): 155 – 160.
- Djajadikerta, H.G., Mat Roni, S. and Trireksani, T. 2015. Dysfunctional information system behaviours are not all created the same: Challenges to the generalizability of security-based research. *Information and Management*, 8-10.

Donalds, C. and Osei-Bryson, K.M. 2020. Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51: 102056.

Donalds, C. and Barclay, C. 2022. Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. *European Journal of Information Systems*, 31(1): 58-73.

Doshi, S. V., Pawar, S.B., Shelar, A. G. and Kulkarni, S. S. 2017. Artificial Intelligence Chatbot in Android System using Open-Source Program-O. *International Journal of Advanced Research in Computer and Communication Engineering*, 6(4): 816–821, April 4.

Egelman, S. Harbach, M. and Peer, E. 2016. Behaviour Ever Follows Intention? A Validation of the Security Behaviour Intentions Scale (SeBIS). *ACM*, 5257–5261.

Egelman, S. and Peer, E. 2015. Scaling the security wall: Developing a security behaviour intentions scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, Seoul, 18-23 April 2015, 2873–2882.

El-Gohary, H.A.S. 2010. The impact of E-marketing practices on market performance of small business enterprises. An empirical investigation. Unpublished Masters Thesis, University of Bradford, Bradford. 4 – 20.

El Hadi Babikir, H., Babikir Ali, A. and El Wahab, M. M. A. 2011. Research Methodology Step by Step Guide for Graduate Students. *Sudanese Journal of Paediatricians*, 9: 9–22.

Eliana, S. 2020. Back to Basics: Towards Building Societal Resilience Against a Cyber Pandemic. *Journal on Systemics, Cybernetics and Informatics (JSCI)*, 18 (7):73-80.

Ertan, A., Crossland, G., Heath, C., Denney, D. and Jensen, R. B. 2018. Everyday Cyber Security in Organizations: A Literature Review. *Academic Centres of Excellence in Cyber Security*, Stratford, June 2018. 5-15.

Eubanks, N., 2017. The true cost of cybercrime for businesses. *Cybercrime-for-businesses*: 7-9.

Evans, M., Maglaras, L.A., He, Y. and Janicke, H. 2016. Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17): 4667-4679.

- Eyisi, D. 2016. The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum. *Journal of Education and Practice*, 7(15): 4 – 8.
- Fagan, M., Albayram, Y., Khan, M.M.H. and Buck, R. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 7(1): 1-20.
- Fellows, R. and Liu, A. 2015. *Research Methods for Construction*. 4th Edition. West Sussex: John Wiley & Sons, 807.
- Fertig, T. and Schütz, A. E. 2020. About the measuring of information security awareness: A systematic literature review. *Proceedings of the Annual Hawaii International Conference on System Sciences*, January 2020, 6518–6527.
- Fiore, D., Baldauf, M. and Thiel, C. 2019. Forgot your password again? - Acceptance and user experience of a chatbot for in-company IT support. *ACM International Conference Proceeding Series*, Pisa, 26-29 November 2019, 2–11.
- Fischer, E. A. 2015. Cybersecurity issues and challenges: In Brief, Cyberspace Threat. *Landscape: Overview, Response Authorities, and Capabilities*, 7: 45–54.
- Flowerday, S. V. and Tuyikeze, T. 2016. Information security policy development and implementation: The what, how and who, *Computers & Security*: 169–183.
- Følstad, A., Nordheim, C. B. and Bjørkli, C. B. 2018. What Makes Users Trust a Chatbot for Customer Service? An Exploratory Interview Study. *Proceedings of the Fifth International Conference on Internet Science 2018*, 2–14.
- Fryer, L. K. and Nakao, K. 2019. Chatbot learning partners: Connecting learning experiences, interest and competence Chatbot learning partners. *Computers in Human Behaviour*: 5-7.
- Fulton, K.R., Gelles, R., McKay, A., Abdi, Y., Roberts, R. and Mazurek, M.L. 2019. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 79-95.
- Gabrielli, S., Marie, K. and Corte, C. D. 2018. SLOW Bot (chatbot) Lifestyle Assistant. *Association for Computing Machinery*: 1–4.

Gandy-Guedes, M.E., Vance, M.M., Bridgewater, E.A., Montgomery, T. and Taylor, K. 2016. Using Facebook as a tool for informal peer support: A case example. *Social Work Education*, 35(3): 323-332.

Gangire, Y., Veiga, A. D. and Herselman, M. 2019. A conceptual model of information security compliant behaviour based on the self-determination theory. *Conference on Information Communications Technology and Society*, 1-6.

Gangire, Y., Veiga, A. D. and Herselman, M. 2020. Information security behaviour: Development of a measurement instrument based on the self-determination theory. *International Symposium on Human Aspects of Information Security and Assurance*, 144-157.

Gangire, Y., Veiga, A. D. and Herselman, M. 2021. Assessing Information Security Behaviour: A self-determination theory perspective. *Information and Computer Security*: 5-6.

Garten, J., Sagae, K., Ustun, V. and Dehghani, M. 2015. Combining distributed vector representations for words. In *Proceedings of the 1st workshop on vector space modeling for natural language processing*, 95-10.

Gemma, R. 2018. Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*: 14-20.

Gerstorf, D., Drewelies, J., Düzel, S., Smith, J., Wahl, H., Schilling, O., Kunzmann, U., Siebert, J., Katzorreck, M., Eibich, P., Demuth, I., Steinhagen-Thiessen, E., Wagner, G., Lindenberger, U., Heckhausen, J. and Ram, N. 2019. Cohort differences in adult-life trajectories of internal and external control beliefs: A tale of more and better maintained internal control and fewer external constraints. *Psychology and Aging*, 34(8): 1090–1108.

Ghose, S. and Barua, J. J. 2017. Toward the implementation of a Topic specific Dialogue based Natural Language Chatbot as an Undergraduate Advisor. *International Conference on Informatics, Electronics and Vision (ICIEV)*, 1–4.

Goel, S., Williams, K., Huang, J. and Warkentin, M. 2020. Understanding the Role of Incentives in Security Behaviour. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 4241–4246.

Goode, J., Levy, Y., Hovav, A. and Smith, J. 2018. Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management*, 6(1): 67–80.

- Goertzen, M.J. 2017. Introduction to quantitative research and data. *Library Technology Reports*, 53(4): 12-18.
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. 2018. Correlating human traits and cyber security behaviour intentions. *Computers & Security*, 73: 345–358.
- Greaves, M., Zibarras, L.D. and Stride, C. 2013. Using the theory of planned behaviour to explore environmental behavioural intentions in the workplace. *Journal of Environmental Psychology*, 34:109-120.
- Guido, B. 2016. Introduction to Quantitative Research. Conference: Kursus Persediaan Ijazah Doktor Falsafah Institut Tadbiran Awam Negara, 7 – 15.
- Gulenko, I. 2014. Chatbot for IT security training: Using motivational interviewing to improve security behaviour. *CEUR Workshop Proceedings*, 7–16.
- Gundu, T. and Flowerday, S.V. 2013. Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, 104(2): 69-79.
- Hadlington, L., Binder, J. and Stanulewicz, N. 2021. Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, 114: 106557.
- Haingura, T. 2019. A Study on Employee Information Security: Human Issue. Unpublished Masters dissertation, Botho University, Gaborone. 11-20.
- Hamdan, B. J. 2013. Evaluating the Performance of Information Security: A Balanced Scorecard Approach. *Association for Information System*, 11: 23-25.
- Hameed, M.A. and Arachchilage, N.A.G. 2020. A conceptual model for the organizational adoption of information system security innovations. In *Security, Privacy, and Forensics Issues in Big Data*: 317-339.
- Han, X. 2020. Am I Asking It Properly?: Designing and Evaluating Interview Chatbots to Improve Elicitation in an Ethical Way. *25th International Conference on Intelligent User Interfaces Companion*, Cagliari, 17-20 March, 33–34.
- Harrell, M. N. 2014. Factors impacting information security noncompliance when completing job tasks. Unpublished PhD Dissertations and Theses, Nova South-eastern University, Florida. 9-20.

- Häußinger, F. 2015. Studies on Employees' Information Security Awareness. Unpublished Dissertation, Göttingen University, Munich. 22-30.
- Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R., Filippoupolitis, A. and Roesch, E. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, 78: 398-428.
- Henderson, S. J. and Feiner, S. K. 2011. Augmented Reality in the Psychomotor Phase of a Procedural Task. *10th IEEE International Symposium on Mixed and Augmented Reality*: 191-200.
- Hengstler, S. and Pryazhnykova, N. 2021. Reviewing the interrelation between information security and culture: Toward an agenda for future research. *16th International Conference on Wirtschaftsinformatik*, 31–56.
- Hengstler, S., Nickerson, R.C. and Trang, S. 2022. Towards a Taxonomy of Information Security Policy Non-Compliance Behavior. In *Proceedings of the 55th Hawaii International Conference on System Sciences*, 7-9.
- Hewitt, B. and White, G. L. 2022. Optimistic Bias and Exposure Affect Security Incidents on Home Computer, *Journal of Computer Information Systems*, 62(1): 50-60.
- Hills, M. and Anjali, A. 2017. A human factors contribution to countering insider threats: Practical prospects from a novel approach to warning and avoiding. *Security Journal*, 30(1): 142-152.
- Hina, S. and Dominic, D. D. 2017. Need for information security policies compliance: A perspective in Higher Education Institutions. *International Conference on Research and Innovation in Information Systems*, 1–11.
- Humaidi, N. and Balakrishnan, V. 2018. Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal 2018*, 47(1): 17–27.
- Hwang, I., Kim, D., Kim, T. and Kim, S. 2017. Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, 41 (1): 2-18.
- Ifinedo, P. and Akinuwesi, B. A. 2014. Employees' Non-Malicious, Counterproductive Computer Security Behaviours (CCSB) in Nigeria and Canada: An Empirical and Comparative Analysis. *IEEE*: 1-7.

- Ifinedo, P. 2015. Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance with Is Security Policy Guidelines. *Information Systems Management*, 33: 1–21.
- Ifinedo, P., Longe, O.B. and Amaunam, I. 2017. Top exemplars of non-malicious, counterproductive computer security behaviours (CCSB) engagements among employees in Nigeria: recommendations for management. *The 8th iSTEAMS, Lagos, Nigeria*, 5-12.
- Ignatov, D. I., Khachay, M. Y., Panchenko, A., Konstantinova, N., Yavorsky, R. and Ustalov, D. 2014. Analysis of Images, Social Networks and Texts. *Supplementary Proceedings of the 3rd International Conference on Analysis of Images, Social Networks and Texts*, Yekaterinburg, April 2014, 7–12.
- Ilker, E. Sulaiman, A. M. and Rukayya, S. A. 2016. Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1): 1 – 4.
- Jaf, S. and Calder, C. 2019. Deep learning for natural language parsing. *IEEE Access*, 7: 131363-131373.
- Jagtap, M. P., Pagar, A. R. and Meshram, T. B. 2018. Cyber Security and Compliance Management through a Single Integrated Platform. *International Journal of Engineering Research & Technology (IJERT)*, 7(9): 57–61.
- Javidi, G. and Sheybani, E., 2018. K-12 cybersecurity education, research, and outreach. In *2018 IEEE Frontiers in Education Conference (FIE)*, 1-5.
- Jerrim, J. and De Vries, R. 2015. The limitations of quantitative social science for informing public policy. *Evidence & Policy: A Journal of Research, Debate and Practice*, 13(1): 117-133.
- Johnson, D.P. 2017. How attitude toward the behavior, subjective norm, and perceived behavioral control affects information security behavior intention. Unpublished PhD dissertation, Walden University, Minneapolis. 80-84.
- Kadir, M. R. A., Norman, S. N. S., Rahman, S. A. and Ahmad, A. R. 2016. Information security policies compliance among employees in Cybersecurity Malaysia. *Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth*, Seville, 2419–2430.

Karlsson, F., Kolkowska, E. and Hedstro, K. 2013. Social action theory for understanding information security non-compliance in hospitals The importance of user rationale. *Information Management & Computer Security*, 21(4): 2-23.

Kaushalya, S.A.D.T.P., Randeniya, R.M.R.S.B. and Liyanage, A.D.S. 2018. An overview of social engineering in the context of information security. In *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 1-6.

Kelley, D. 2018. Investigation of Attitudes Towards Security Behaviours. *McNair Research Journal SJSU*, 14: 12-25.

Khan, H. U. and Alshare, K. A. 2019. Violators versus non-violators of information security measures in organizations — A study of distinguishing factors, *Journal of Organizational Computing and Electronic Commerce*, 29(1): 4–23.

Khonji, M. 2013. Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, 15(4): 2091 – 2121.

Kim, S. S. and Kim, Y. J. 2020. The effect of compliance knowledge and compliance support systems on information security compliance behaviour. *Journal of Knowledge Management*, 21(4): 2-26.

Kirlappos, I., Beautement, A. and Sasse, M. A. 2013. Comply or Die “: Long live security aware principal agents. *The need for Information Security*: 2-15.

Kirlappos, I., Parkin, S. and Sasse, M. A. 2014. Learning from “Shadow Security”: Why understanding non-compliant behaviours provides the basis for effective security. *Internet Society*: 1–10.

Kolkowska, E., Karlsson, F. and Hedström, K. 2017. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *Journal of Strategic Information Systems*, 6: 39–57.

Kottorp, M. and Jaderberg, F. 2017. Chatbot as a potential tool for businesses. *SVERIGE*: 4–20.

Kousa, E. 2019. Exploring Success Factors in Chatbot Implementation Projects. Unpublished Masters thesis, Acada University, Helsinki. 10–17.

Kowalski, S., Pavlovska, K. and Goldstein, M. 2013. Two Case Studies in Using Chatbots Quick Overview of Security Awareness Training. *International Federation for Information Processing*: 265–272.

Kretzer, M. and Maedche, A. 2015. Which are the Most Effective Measures for Improving Employees' Security Which are the Most Effective Measures for Improving Employees' Security Compliance? Completed Research Paper. *Thirty Sixth International Conference on Information Systems*, Fort Worth, December 2015. 2-18.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. 2015. Advanced social engineering attacks. *Journal of Information Security and applications*, 22: 113-122.

Kumar, R. 2011. *Research Methodology a step-by-step guide for beginners*. 3rd edition. New Dehli: SAGE Publications. 10-105.

Kuppusamy, P., Samy, G.N., Maaropa, N., Magalingama, P., Kamaruddina, N., Shanmugamb, B. and Perumalc S. 2020. Systematic Literature Review of Information Security Compliance Behaviour Theories. *Journal of Physics*: 3-8.

Leshem, S. and Trafford, V. 2007. Overlooking the conceptual framework, *Innovations in Education and Teaching International*, 44(1): 93–105.

Liechti, O. and Sumi, Y. 2002. Awareness and the WWW. *International Journal of Human-Computer Studies*, 56(1): 1-5.

Liu, C., Wang, N. and Liang, H. 2020. Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, 54(28): 102-152.

Linkov, V., Zámečník, P., Havlíčková, D. and Pai, C.W. 2019. Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in Psychology*, 10: 995.

Lommatzsch, A. 2018. A Next Generation Chatbot-Framework for the Public Administration. *Distributed Artificial Intelligence Laboratory*: 1–12.

Lorenzo, N. and Gallon, R. 2019. Smart pedagogy for smart learning. In *Didactics of smart pedagogy*: 41-69.

- Louanglath, P. I. 2017. Minimum Sample Size Method Based on Survey Scales. *International Journal of Research & Methodology in Social Science*, 3(3): 45-46.
- Lowry, P. B. 2017. Cognitive-affective drivers of employees ' daily compliance with information security policies: A multilevel, longitudinal Study. *Information Systems Journal (ISJ)*: 4-12.
- Luh, R., Marschalek, S., Kaiser, M., Janicke, H. and Schrittwieser, S., 2017. Semantics-aware detection of targeted attacks: a survey. *Journal of Computer Virology and Hacking Techniques*, 13(1):47-85.
- Lyons, K. 2017. Intelligent Chatbot: Technical Report. Unpublished Doctoral dissertation, National College of Ireland, Dublin. 53–64.
- MacDonald, S and Headlam, N. 2011. *Research Methods Handbook: Introductory guide to research methods for social research*. Manchester: Centre for Local Economic Strategies. 5 – 25.
- Mack, N., Woodsong, C., MacQueen, K.M., Guest, G. and Namey, E. 2005. *Qualitative Research Methods: A Data Collector's Field Guide*. Durham: Family Health International. 5 – 12.
- Maennel, K., Mäses, S. and Maennel, O., 2018. Cyber hygiene: The big picture. In *Nordic Conference on Secure IT Systems*: 291-305.
- Mahfuth, A., 2019. Human factor as insider threat in organizations. *International Journal of Computer Science and Information Security (IJCSIS)*, 17(12): 7-9.
- Mai, N.E.O., 2022. The Merlin Project: Malaysian Students'acceptance of An Ai Chatbot in Their Learning Process. *Turkish Online Journal of Distance Education*, 23(3): 31-48.
- Majid, U. 2018. Research Fundamentals: Study Design, Population, and Sample Size. *URNCSST Journal*, 2(1): 5-7.
- Majumder, S. and Mondal, A., 2021. Are chatbots really useful for human resource management? *International Journal of Speech Technology*, 24(4):969-977.
- Malhotra, R. 2015. A systematic review of machine learning techniques for software fault prediction. *Applied Soft Computing Journal*: 6-25.

- Malhotra, G. 2017. Strategies in Research. *International Journal of Advance Research and Development*, 2(5): 173 – 174.
- Malvisi, F. 2014. Development of a Framework for AIML Chatbots in HTML5 and Javascript. Unpublished final thesis, Linköping University, Linköping. 2–50.
- Manju, K. and Mathur, B. 2014. Data Analysis of Students' Marks with Descriptive Statistics. *International Journal IJRITCC*: 2-5
- Marble, J.L., Lawless, W.F., Mittu, R., Coyne, J., Abramson, M. and Sibley, C., 2015. The human factor in cybersecurity: Robust & intelligent defense. In *Cyber warfare*:173-206.
- Marczyk, G., DeMatteo, D. and Festinger, D. 2005. *Essentials of Research Design & Methodology*. New Jersey: John Wiley & Sons, Inc. 158-200.
- Maynard, S., Tan, T., Ahmad, A. and Ruighaver, T. 2018. Towards a framework for strategic security context in information security governance. *Pacific Asia Journal of the Association for Information Systems*, 10(4): 4.
- McCusker, K. and S Gunaydin, S. 2016. Research using qualitative, quantitative or mixed methods and choice based on the research. *JAMA*: 5 – 10.
- Melnyk, K. P. and Shmatkovska, T.O. 2016. Fundamentals of the Theory and Methodology of Operational Control. *British Journal of Economics, Management & Trade*, 14(4): 1-12.
- McSweeney, K. 2018. Motivating cybersecurity compliance in critical infrastructure industries: A grounded theory study, Unpublished Dissertation, Capella University, Minnesota. 20-25.
- 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): 1203-1230.
- Merhi, M. I. and Midha, V. 2012. The Impact of Training and Social Norms on Information Security Compliance. *IS Security and Privacy*, 5: 2-11.
- Meyer von Wolff, R., Hobert, S. and Schumann, M. 2019. How May I Help You? State of the Art and Open Research Questions for Chatbots at the Digital Workplace. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 95–104.

- Milov, O., Kostyak, M., Milevskiy, S. and Rzaev, H.N.O. 2019. Information security investment model: resource representation and organizational training. *Advanced Information Systems*, 3(4): 96-104.
- Mitchell, L. M. and Jolley, M. J. 2010. *Research Design Explained*. 7th Edition. Wadsworth: Cengage Learning. 6-11.
- Moody, G.D., Siponen, M. and Pahlila, S. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly*: 42(1).
- Moraes, N. A., and Márcia, F. 2019. Chatbot and Conversational Analysis to Promote Collaborative Learning in Distance Education. *IEEE 19th International Conference on Advanced Learning Technologies*, Maceio, 324-326.
- Muhammad, K. S. 2016. *Basic Guidelines for Research: An Introductory Approach for All Disciplines*. 1st Edition. Chittagong: Book Zone Publication. 201-275.
- Muijs, D. 2015. *Quantitative research, Nursing standard*. London: SAGE Publications. 31-45.
- Mwagwabi, F., McGill, T. and Dixon, M. 2014. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. *Proceedings of the Annual Hawaii International Conference on System Sciences*, Waikoloa, 3188–3197.
- Nair, G. and Johnson, S. 2018. Chatbot as a Personal Assistant. *International Journal of Applied Engineering Research*, 13(20): 14644–14649.
- Nasir, A. & Fahmy, S. 2021. Information Security Culture Concept towards Information Security Compliance: A Comparison between IT and Non-IT Professionals. *International Conference on Digital Transformation in Technology, Engineering and Management*, Johor, 5-16.
- Ngoqo, B. and Flowerday, S. V. 2015. Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security*, 53: 132–142, June.
- Nicholson, J., Coventry, L. and Briggs, P. 2019. "If It's Important It Will Be a Headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-11.

- Nordberg, O. E., Wake, J. D., Flobak, E., Nordgreen, T., Mukhiya, S. K. and Guribye, F. 2019. Designing Chatbots for Guiding Online Peer support Conversations for Adults with ADHD. *Conversations 2019*, Amsterdam, 1–14.
- Oates, B. 2006. *Researching information systems and computing*. London: SAGE Publications, 33-34.
- Oduntan, O. and Adegboye, O. 2017. Enhancing Communication Technology Through an Intelligent. *National Media Communication & IT Conference for Tertiary Institutions*, Ogun, 1–12.
- Ogunnoiki, C. 2019. The Impact of Reward, Penalty, Security Training Programs, Social Pressures, and Job Satisfaction on Security Behaviours Among Healthcare Workers: A Correlational Study. Unpublished PhD Dissertation, Capella University, Minneapolis. 8-10.
- Okonkwo, C. W and Ade-Ibijola, A. 2021. Chatbots applications in education: A systematic review. *Computers and Education: Artificial Intelligence*, 2: 6-9.
- Omidosu, J. and Ophoff, J. 2017. A theory-based review of information security behaviour in the organization and home context. *Proceedings - 2016 3rd International Conference on Advances in Computing, Communication and Engineering*, Durban, 28-29 November, 225–231.
- Padayachee, K. 2012. Taxonomy of compliant information security behaviour, *Computers & Security*: 1–8.
- Paikari, E. and Van Der Hoek, A. 2018. A framework for understanding chatbots and their future. *Proceedings - International Conference on Software Engineering*, Gothenburg, 27 May, 13–16.
- Park, Y. S., Lars, K. and Artino, A. R. 2019. The Positivism Paradigm of Research. *Academic Medicine. Journal of the Association of American Medical Colleges*: 691 – 695.
- Park, D., Bahrudin, F. I. and Han, J. 2020. Circular Reasoning for the Evolution of Research Through a Strategic Construction of Research Methodologies. *International Journal of Quantitative and Qualitative Research Methods*, 8(23): 1 – 23.
- Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B. and Wang, G. 2019. What happens after you leak your password: Understanding credential sharing on phishing sites. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 181-192.

- Pham, H.C., El-Den, J. and Richardson, J. 2016. Stress-based security compliance model an exploratory study. *Information & Computer Security*: 12-15.
- Pham, H. C., Brennan, L., and Richardson, J. 2017. Review of Behavioural Theories in Security. *Proceeds of the Information Science + Information Technology Education Conference*, Saigon, July 31 - August 5, 65-76.
- Pham, H. C., Pham, D.D., Brennan, L. and Richardson, L. 2017. Information Security and People: A Conundrum for Compliance. *Information Security & People*, 21: 1–16.
- Pigliacelli, F. 2020. Smart speakers' adoption: Technology Acceptance Model and the role of Conversational Style. Unpublished Masters Thesis, Luiss University, Rome. 8-10.
- Podesva, R. J. and Sharma, D. 2013. *Research Methods in Linguistics*. Cambridge: Cambridge University Press. 10-50.
- Puhakainen, P. and Siponen, M. 2015. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*: 16-22.
- Quagliata, K. 2012. Impact of Security Awareness Training Components on Security Effectiveness. *National Institute of Standards and Technology*: 3-17.
- Queirós, A., Faria, D. and Almeida, F. 2017. Strengths and Limitations of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*, 3(9): 369 – 380.
- Rader, E. and Wash, R. 2015. Identifying Patterns in Informal Sources of Security Information. *Journal of Cybersecurity*, 1(1): 121–144.
- Rahman, M.S. 2020. The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “testing and assessment” research: A literature review. *Journal of Education and Learning*, 6(1): 102 – 115.
- Rai, N. and Thapa, B. 2015. A study on purposive sampling method in research. *Kathmandu School of Law*: 1-12.
- Rajasooriya, S.M., Tsokos, C.P. and Kaluarachchi, P.K. 2017. Cyber security: Nonlinear stochastic models for predicting the exploitability. *Journal of Information Security*, 8(02): 125

- Ranoliya, B. R., Raghuwanshi, N. and Singh, S. 2017. Chatbot for University-Related FAQs. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, 1525–1530.
- Rao, Y. S., Pradhan, D., Panda, T. C. and Rath R. 2020. Digital Crime and its Impact in Present Society. *International Journal of Engineering Research & Technology (IJERT)*: 3-6.
- Ray, J.R. 2014. Training Programs to Increase Cybersecurity Awareness and Compliance in Non-profits. Unpublished Masters thesis, University of Oregon, Oregon, December. 4-15.
- Richardson, M. D., Lemoine, P. A., Stephens, W. E. and Waller, R. E. 2020. Planning for Cyber Security in Schools: The Human Factor: Roadrunner Search Discovery Service. *Educational Planning*, 27(2): 17.
- Robinson, C. 2019. Impressions of Viability: How Current Enrolment Management Personnel and Former Students Perceive the Implementation of a Chatbot Focused on Student. *Higher Education Doctoral Projects*: 47–56.
- Rubesch, T. 2013. Designing an Embodied Conversational Agent for a Self-Access Center. *Language Education and Research*, 23: 171-182.
- Ruighaver, A. B., Maynard, S. B. and Warren, M. 2012. Towards Understanding Deterrence: Information Security Manager's Perspective. *Proceeds of the International Conference on IT Convergence and Security*, 1–8.
- Rupere, T. and Muhonde, M. 2012. Towards Minimizing Human Factors in End-User Information Security. *Journal of Information Security Research*, 3(4): 171-183, December.
- Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J. 2017. A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253-259.
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. and Herawan, T. 2015. Information security conscious care behaviour com formation in organizations. *Computers & Security*: 65–78.
- Safa, N. S., Von Solms, R. and Furnell, S. 2016. Information security policy compliance model in organizations', *Computers and Security*: 1–13.

- Safa, N.S., Maple, C., Furnell, S., Azad, M.A., Perera, C., Dabbagh, M. and Sookhak, M. 2019. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, 97: 587-597.
- Salkind, N. J. 2012. *Exploring Research*. 8th Edition. New York: Pearson, 407.
- Sanders, G.L., Upadhyaya, S. and Wang, X. 2019. Inside the insider. *IEEE Engineering Management Review*, 47(2): 84-91.
- Sandu, N. and Gide, E. 2019. Adoption of AI-Chatbots to Enhance Student Learning. *Experience in Higher Education in India: 2-7*.
- Sannikova, S. 2018. Chatbot implementation with Microsoft Bot Framework. Unpublished Bachelor thesis, Metropolia University, Helsinki. 5-8.
- Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A. 2020. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, 7(1): 1-29.
- Schütz, A.E., 2018. Information security awareness: it's time to change minds. In Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development-ICDD, 44-45.
- Shah, S. and Shah, S. 2019. A comparison of various chatbot frameworks. *J. Multi-Criteria Decis. Anal*, 6: 375-383.
- Sharma, G. 2017. Pros and cons of different sampling techniques Gaganpreet. *International Journal of applied research*, 3(7): 749–752.
- Sharma, V., Goyal, M. and Malik, D. 2017. An Intelligent Behaviour Shown by Chatbot System. *International Journal of New Technology and Research (IJNTR)*, 3(4): 52–54, April.
- Shen, K. N. 2016. Understanding Bring Your Own Device (BYOD) and Employee Information Security Behaviours from A Work-Life Domain Perspective. *Twenty-second Americas Conference on Information Systems*, San Diego, 1–10.
- Sherly, A. 2011. Information Security Behaviour: Factors and Research Directions. *AMCIS 2011: 2-3*.

- Sherly, A. and Lifang, S. 2015. Towards an integrative learning approach in cybersecurity education. *Information Security Education Journal*, 2(2): 5-7.
- Shillair, R. and Meng, J. 2017. Multiple sources for security: The influence of source networks on coping self-efficacy and protection behavior habits in online safety. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4977–4986.
- Shrestha, P. and Thakur, R. N. 2019. Study on Security and Privacy Related Issues Associated with BYOD Policy in Organizations in Nepal. *LBEF Research Journal of Science, Technology and Management*, 1(2): 4-6.
- Shull, F., Singer, J. and Sjøberg, D. I. K. 2008. Guide to advanced empirical software engineering, *Guide to Advanced Empirical Software Engineering*: 5-30.
- Siddiqui, R. A. 2015. Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 3(1): 2-5.
- Simonet, J. and Teufel, S. 2019. The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In *IFIP international conference on ICT systems security and privacy protection*, 194-208.
- Simpson, C. J. 2019. Unauthorized Disclosures of Sensitive and Classified Information: A Meta-Synthesis Of Leadership Support, Security Policy, and Security Education, Training and Awareness Within the Federal Government Information Security Culture. Unpublished PhD Dissertation, Delaware State University, Dover. 18-30.
- Singh, Y.K. 2006. *Fundamental of Research Methodology and Statistics*. New Dehli: New Age International Publishers, 52-70.
- Singh, A. S. and Masuku, M. B. 2013. Fundamentals of Applied Research and Sampling Techniques. *International Journal of Medical and Applied Sciences*, 2(4): 124 – 130.
- Singh, A.S. and Masuku, M. B. 2014. Sampling Techniques & Determination of Sample Size in Applied Statistics Research: An Overview. *International Journal of Economics, Commerce and Management*, 2(11): 2 – 8.
- Sivaranjani, M. 2020. The Extendibility Of Artificial Intelligence In The Human Resource Management. *UGC Care Listed Journal Studies*, 40(16): 601-607.

- Sommer, L. 2011. The theory of planned behaviour and the impact of past behaviour. *International Business & Economics Research Journal (IBER)*, 10(1) 9-12.
- Soomro, Z. A., Shah, M. H. and Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*: 215–225.
- Spross, J. 2014. A Critical Review of the Observational. Unpublished Master's thesis, KTH Royal Institute of Technology, Stockholm. 7-10.
- Stanciu, V. and Tinca, A. 2017. Exploring cybercrime realities and challenges. *Journal of Accounting and Management Information Systems*, 16(4): 610–632.
- Sukamolson, S. 2007. Fundamentals of quantitative research. Unpublished PhD dissertation, Chulalongkorn University, Bangkok. 1 – 20.
- Suta, P., Lan, X., Wu, B., Mongkolnam, P. and Chan, J.H. 2020. An overview of machine learning in chatbots. *Int J Mech Engineer Robotics Res*, 9(4): 502-510.
- Sveen, K. 2016. Leverage Efficiency with Optimised Information Security Communication. Unpublished Masters thesis, Norwegian University of Science and Technology, Trondheim. 16-25.
- Taherdoost, H. 2016. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)*, 20: 2-4.
- Tam, K. and Jones, K. 2019. A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1): 129-163.
- Tangkittipon, P., Sawatdirat, A., Lakkhanawannakun, P. and Noyunsan, C. 2020. Facilitating A Flipped Classroom using Chatbot: A Conceptual Model. *Engineering Access*, 6(2):103-107.
- Taylor, P.C. and Medina, M. 2011. Educational research paradigms: from positivism to pluralism. *College Research Journal*, 1(1): 1-16.
- Tenzin, S., 2021. An investigation of the factors that influence information security culture in government organisations in Bhutan. Unpublished PhD dissertation, Murdoch University, Perth. 52-56.

Thies, I. M., Menon, N., Magapu, S., Subramony, S. and O'Neill, J. 2017. 'How do you want your chatbot? An exploratory Wizard-of-Oz study with young, urban Indians. *IFIP Conference on Human-Computer Interaction*, 1-18.

Thorat, S.A. and Jadhav, V., 2020. A review on implementation issues of rule-based chatbot systems. In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 8-10.

Tolah, A., Furnell, S.M. and Papadaki, M. 2021. An empirical analysis of the information security culture key factors framework. *Computers & Security*, 108: 102354.

Topa, I. and Karyda, M. 2016. Analysing security behaviour determinants for enhancing ISP compliance and security management. *Proceedings of the 13th European, Mediterranean and Middle Eastern Conference on Information Systems*, Krakow, 23-24 June. 423–435.

Varitimiadis, S., Kotis, K., Skamagis, A., Tzortzakakis, A., Tsekouras, G. and Spiliotopoulos, D. 2020. Towards implementing an AI chatbot platform for museums. In *International Conference on Cultural Informatics, Communication & Media Studies*, 1(1), 8-10.

Vedadi, A. and Warkentin, M. 2018. Secure Behaviour over Time: Perspectives from the Theory of Process Memory. *DATABASE for Advances in Information Systems*, 49: 39–48.

Villegas-Ch, W., Arias-Navarrete, A. and Palacios-Pacheco, X. 2020. Proposal of an Architecture for the Integration of a Chatbot with Artificial Intelligence in a Smart Campus for the Improvement of Learning. *Sustainability*, 12(4): 5–10.

Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. 2018, May. Hackers vs. testers: A comparison of software vulnerability discovery processes. In *2018 IEEE Symposium on Security and Privacy (SP)*, 374-391.

Wang, S. and Wang, H. 2019. Opportunities and challenges of cybersecurity for undergraduate information systems programs. *International Journal of Information and Communication Technology Education (IJICTE)*, 15(2): 49-68.

Warkentin, M. and Baskerville, R. 2013. Future directions for behavioural information security research Future directions for behavioural information security research. *Computers & Security*: 90–101.

Warkentin, M., Johnston, A. C., Shropshire, J. and Barnett, W. D. 2016. Continuance of protective security behaviour: *Decision Support Systems*, 92: 25–35.

- Wash, R. and Rader, E. 2019. Too much knowledge? Security beliefs and protective behaviours among United States internet users. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*, Ottawa, 22-24 July. 309–325.
- Wash, R., Nthala, N. and Rader, E. 2021. Knowledge and Capabilities that Non-Expert Users Bring to Phishing Detection. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*, Michigan, 10-14.
- Welman, C., Kruger, F. and Mitchell, B. 2005. *Research Methodology*. Third Edition. Cape Town: Oxford University Press, 54-80.
- Whitman, M.E. and Mattord, H.J. 2021. *Principles of information security*. 7th Edition. Boston: Cengage learning. 82-87.
- Wilson, V. 2014. Research Methods: Sampling. *Evidence Based Library and Information Practice*, 9(2): 45 – 50.
- Winkler, R. and Söllner, M. 2018. Unleashing the Potential of Chatbots in Education: A State-Of-The-Art Analysis. *Academy of Management Annual Meeting (AOM)*: 2-30.
- Woiceshyn, J. and Daellenbach, U. 2018. Evaluating Inductive versus Deductive Research in Management Studies: Implications for Authors, Editors, and Reviewers. *Qualitative Research in Organizations and Management An International Journal*: 2-6.
- Wynn, D., Karahanna, E., Williams, C. K. and Madupalli, R. 2013. Preventive Adoption of Information Security Behaviours. *Thirty Third International Conference on Information Systems*, Orlando, 1–18.
- Yan, Z., Xue, Y. and Lou, Y. 2021. Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, 121: 106791.
- Yaokumah, W. and Kumah, P. 2018. Exploring the Impact of Security Policy on Compliance. *IGI Global Journals*: 3-5.
- Yen, C. and Chiang, M.C. 2021. Trust me, if you can: a study on the factors that influence consumers' purchase intention triggered by chatbots based on brain image evidence and self-reported assessments. *Behaviour & Information Technology*, 40(11): 1177-1194.

- Yıldırım, M. and Mackie, I. 2019. Encouraging users to improve password security and memorability. *International Journal of Information Security*, 18(6): 741–759.
- Young, H., Vliet, T.V., Ven, J.V.D., Jol, S. and Broekman, C. 2017. Understanding human factors in cyber security as a dynamic system. In *International Conference on Applied Human Factors and Ergonomics*, 244-254.
- Zeng, E., Mare, S. and Roesner, F. 2017. End User Security and Privacy Concerns with Smart Homes. *Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, 12-14 July. 65–80.
- Zimmermann, V. and Renaud, K. 2019. Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131: 169-187.
- Zumstein, D. and Hundertmark, S. 2018a. Chatbots: an interactive technology for personalized communication and transaction. *IADIS International Journal*, 15(1): 100–104.
- Zumstein, D. and Hundertmark, S. 2018b. Chatbots an Interactive Technology for Personalized Communication, Transactions and Services. *IADIS International Journal*, 15(2): 96–109.

APPENDICES

Appendix A: Ethics Approval Letter



PO Box 1906, Belville, 7535 | Symphony Way, Belville, Cape Town, South Africa
+27 (0)21 959 6767 | www.facebook.com/cput.ac.za | info@cput.ac.za | www.cput.ac.za

Office of the Research Ethics Committee
Faculty of Informatics and Design
Room 2.09
80 Roeland Street
Cape Town
Tel: 021-469 1012
Email: ndedem@cput.ac.za
Secretary: Mziyanda Ndede

21 September 2021

Goodman Mzwabantu Siyongwana
c/o Department of Information Technology
CPUT

Reference no: 208225609 /2021/28

Project title: Enforcement of end-user compliance using chatbot

Approval period: 21 September 2021 – 31 December 2022

This is to certify that the Faculty of Informatics and Design Research Ethics Committee of the Cape Peninsula University of Technology approved the methodology and ethics of Goodman Mzwabantu Siyongwana (208225609) for the MTech Information Technology.

Any amendments, extension or other modifications to the protocol must be submitted to the Research Ethics Committee for approval.

The Committee must be informed of any serious adverse event and/or termination of the study.



A/Prof I van Zyl
Chair: Research Ethics Committee
Faculty of Informatics and Design
Cape Peninsula University of Technology

Appendix B: Cyber Security Standards

Cyber Security Standards	Description
International Organization for Standardization (ISO)	ISO is the leading developer of international standards
International Electrotechnical Commission (IEC)	IEC works closely with ISO
National Institute of Standards and Technology (NIST)	NIST is a non-regulatory information security standards developer
Internet Engineering Task Force (IETF)	IETF deals with technical standards and Internet protocol suite (TCP/IP)
Information Security Forum (ISF)	ISF is responsible for advancing good information security practices
Institute of Information Security Professionals (IISP)	IISP is responsible for maintaining the professional standards of security practitioners and the entire information security industry