TOWARDS A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS

by

MATHIAS MUJINGA
47513098

submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY

in the subject of

COMPUTER SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. M.M. ELOFF
CO-SUPERVISOR: PROF. J.H. KROEZE

JANUARY 2018

DECLARATION

I declare that "TOWARDS A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS" is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

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

…………………………….	30 JANUARY 2018…..
Signature	Date

ACKNOWLEDGEMENTS

Firstly, I would like to thank my supervisors, Prof Mariki M. Eloff and Prof Jan H. Kroeze, whose guidance during the course of this study was invaluable. I say thank you from the bottom of my heart for your support, guidance, and assistance during this journey.

Secondly, I would like to thank all those who participated in this research as survey respondents, interview participants, and framework evaluators. I also want to extend my gratitude to the language editor, Ms H Baker; the statistician, Mr E Kademeteme; and the transcriber, Mr P Mekgwe, your services are much appreciated.

Last, but not least, I would like to take this opportunity to thank my wife, Landie, my son, Ethan, my parents, my siblings, my friends, and my colleagues for their support throughout.

ABSTRACT

The proliferation of the internet and associated online activities exposes users to numerous information security (InfoSec) threats. Such online activities attract a variety of online users who include novice computer users with no basic InfoSec awareness knowledge. Information systems that collect and use sensitive and confidential personal information of users need to provide reliable protection mechanisms to safeguard this information. Given the constant user involvement in these systems and the notion of users being the weakest link in the InfoSec chain, technical solutions alone are insufficient. The usability of online InfoSec systems can play an integral role in making sure that users use the applications effectively, thereby improving the overall security of the applications.

The development of online InfoSec systems calls for addressing the InfoSec problem as a social problem, and such development must seek to find a balance between technical and social aspects. The research addressed the problem of usable security in online InfoSec applications by using an approach that enabled the consideration of both InfoSec and usability in viewing the system as a socio-technical system with technical and social sub-systems. Therefore, the research proposed a socio-technical framework that promotes the development of usable security for online information systems using online banking as a case study.

Using a convergent mixed methods research (MMR) design, the research collected data from online banking users through a survey and obtained the views of online banking developers through unstructured interviews. The findings from the two research methods contributed to the selection of 12 usable security design principles proposed in the socio-technical information security (STInfoSec) framework.

The research contributed to online InfoSec systems theory by developing a validated STInfoSec framework that went through an evaluation process by seven field experts. Although intended for online banking, the framework can be applied to other similar online InfoSec applications, with minimum adaptation. The STInfoSec framework provides checklist items that allow for easy application during the development process. The checklist items can also be used to evaluate existing online banking websites to identify possible usable security problems.

LIST OF PUBLICATIONS

The following is a list of peer-reviewed publications published during the course of this research.

1. Mujinga, M., Eloff, M.M. & Kroeze, J.H. (2018). ‘System usability scale evaluation of online banking service: a South African study’, South African Journal of Science, vol. 114, no. 3/4, pp. 50-57. https://doi.org/10.17159/sajs.2018/20170065.
2. Mujinga, M., Eloff, M.M. & Kroeze, J.H. (2017). ‘A socio-technical approach to information security’, Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA, 10-12 August 2017, ISBN: 978-0-9966831-4-2.
3. Mujinga, M., Eloff, M.M. & Kroeze, J.H. (2016). ‘Online banking users’ perceptions in South Africa: An exploratory empirical study’, Proceedings of the IST-Africa 2016 Conference, Durban, SA, 11-13 May 2016, ISBN: 978-1-905824-54-0.
4. Mujinga, M., Eloff, M.M. & Kroeze, J.H. (2013). ‘Towards a heuristic model for usable and secure online banking’, Proceedings of the 24th Australasian Conference on Information Systems (ACIS), Melbourne, Australia, 4-6 December 2013, ISBN: 978-0-9924495-0-6.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

2FA	Two-factor authentication
3FA	Three-factor authentication
APWG	Anti-Phishing Working Group
ARPA	Advanced Research Projects Agency
ATM	Automated teller machine
BASA	Banking Association of South Africa
B2B	Business-to-business
B2C	Business-to-consumer
B2G	Business-to-government
C2B	Consumer-to-business
C2C	Consumer-to-consumer
CAQDAS	Computer-assisted qualitative data analysis software
CFA	Confirmatory factor analysis
CFI	Comparative fit index
CIA	Confidentiality, integrity, and availability
CR	Critical ratio
Ebanking	Electronic banking
Ebusiness	Electronic business
Ecommerce	Electronic commerce
EU	European Union
EFA	Exploratory factor analysis
EFT	Electronic funds transfer
G2B	Government-to-business
G2C	Government-to-citizen
GDP	Gross domestic product
GFI	Goodness-of-fit index
HCI	Human-computer interaction
HCISec	Human-computer interaction security
HTTP	Hypertext Transfer Protocol
ICT	Information communication technology
IEA	International Ergonomics Association
IEC	International Electrotechnical Commission
IITF	Information Infrastructure Task Force

InfoSec	Information security
IS	Information system
ISO	International Organization for Standardization
IT	Information technology
IXD	Interaction design
MMR	Mixed methods research
OTP	One-time password
PCA	Principal component analysis
PIN	Personal identification number
RMSEA	Root mean square error of approximation
S-HTTP	Secure Hypertext Transfer Protocol
SABRIC	South African Banking Risk Information Centre
SABS	South African Bureau of Standards
SEM	Structural equation modelling
SFA	Single-factor authentication
SMS	Short message service
SNS	Social network site
SPSS	Statistical Package for the Social Sciences
SRMR	Standardised root mean square residual
SSL	Secure Sockets Layer
STM	Short-term memory
STS	Socio-technical systems
SUS	System usability scale
TLS	Transport Layer Security
UCD	User-centred design
UN	United Nations
UTAUT	Unified theory of acceptance and use of technology
UX	User experience

KEYWORDS

Information security, Usable security, Socio-technical, Online banking, STInfoSec, Design principles, User behaviour, South Africa, Heuristic evaluation, Mixed methods research

CHAPTER 1 INTRODUCTION

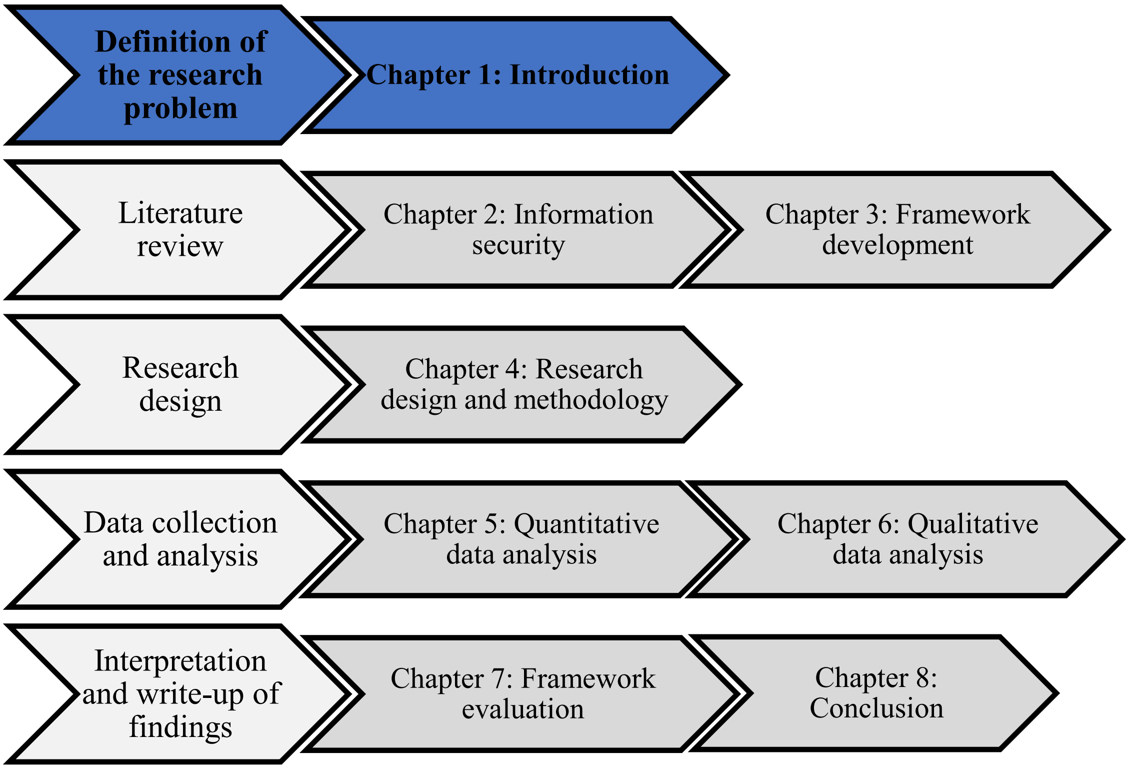

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 1-1: The research roadmap

1.1 INTRODUCTION

The internet and other technological services have transformed how individuals and private or public organisations conduct their business; all have subsequently evolved to incorporate some form of online communication technology. With the internet as medium for information dissemination, organisations and individuals are becoming progressively more reliant on electronic information and distribution of information. However, being an open and public medium, the internet brings about new risks and threats to the confidentiality, integrity, and availability of information. The internet initially had a single objective of a free and open exchange of information, as it was developed during a period when users and hosts were mutually trusting (Oppliger 1997). Since then, the expansion of internet usage beyond the boundaries of trust and security has meant that security of information in transit and storage has become critical to achieving organisational goals.

Today, the internet is plagued with a variety of malicious software, commonly referred to as malware, as well as other cyberthreats. Malware is any additional code added to, changed from or removed from, a software system to intentionally cause harm or subvert the intended function of the system (He, Chan & Guizani 2015). Malware attacks computer systems and gathers sensitive information such as credit card numbers and passwords (He et al. 2015). As such, online information systems are at risk of personal and confidential information being accessed by these unauthorised entities that carry out malware attacks.

1.1.1 Information security

Electronic commerce (ecommerce) websites and other related technologies rely on web browser technology to access internet content from a multitude of devices. However, the proliferation of smartphones has brought about a variety of applications that provide internet content directly through smartphone apps without the use of the 'traditional' web browser application. The web browser is still the primary means of accessing internet content from desktop and portable (laptop) computers, including smartphones. Browser security can only protect users against certain types of attacks through additional security, depending on users' vigilance, such as avoiding sending sensitive information through unsecure web browser sessions.

Ecommerce is the buying and selling of information, products, or services over an electronic channel such as the internet or an intranet (Turban, King, Lee, Liang & Turban 2015). Significantly, ecommerce has revolutionised the way organisations and governments do business and how individuals perform their day-to-day lifestyle activities. This has evolved into a number of industries, with the emergence of terms such as 'elearning', 'ehealth', 'egovernment', and 'ebanking', were 'e' refers to 'electronic'. However, with the widespread adoption of ecommerce, the data transmitted through ecommerce channels include sensitive and confidential information such as personal and financial details. Consequently, with the internet being open, it is important to protect data in transmission against unauthorised access or modification. Hence, information security (InfoSec) has become an integral part of the success or failure of ecommerce.

There have been significant advances in the technical aspects of systems security for protecting confidential information and data in storage and transmission (Choo 2011b). These include the use of data encryption standards, firewalls, intrusion detection systems, and biometric devices (Mitnick & Simon 2005). Unfortunately, any information system is only as secure as its weakest link, and InfoSec attacks normally look for the path of

least resistance. It is generally acknowledged that users are the weakest link in the InfoSec chain (Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville 2013). Since most systems rely on the actions of users, the weaknesses brought about by user interactions with the systems usually erode the technical gains.
The Oxford Dictionary (2018) defines security as "*the state of being or feeling secure*" and information as "*what is conveyed or represented by a particular arrangement or sequence of things*". In computing terms, the phrase 'information security' has become common. Depending on one's viewpoint, there are many definitions of InfoSec, as it can be viewed from a technical, behavioural, managerial, philosophical, and/or organisational perspective (Zafar & Clark 2009).

If viewed as a social science that examines the behaviour of individuals as they interact with systems, InfoSec begins and ends with the people inside and outside the organisation who interact with the system (Whitman & Mattord 2017). Dhamija & Perrig (2000) argue that systems should be evaluated not only theoretically, but also by how secure they are in common practice. Parsons, McCormac, Butavicius, and Ferguson (2010) affirm that for InfoSec to adequately provide protection to information assets it has to consider how human users will interact with the system. Nevertheless, designers do not always take human cognitive limitations into consideration when designing and evaluating information system security (Dhamija & Perrig 2000).

What is certain, however, is that organisations have to guard against InfoSec threats from both outsiders and insiders when protecting organisational digital assets and that major threats come from insiders (Hu, Dinev, Hart & Cooke 2012). Recent surveys from technical reports regarding InfoSec and empirical research studies suggest that more damaging breaches are caused by the actions of internal employees than outside hackers (Crossler et al. 2013). It is worth noting that most insider threats are not considered intentional, but unintentional mistakes (Stanton & Stam 2006). Hence, it is vital to address the causes of such unintentional mistakes, and a usable system goes a long way to mitigate these mistakes.

InfoSec and privacy are among the major concerns of consumers when making ecommerce and online banking adoption decisions (Adapa & Cooksey 2013, Yousafzai & Yani-de-Soriano 2012). Technical reports compiled by security, risk, and insurance organisations identify the importance of internet security, citing an increase in hackers and attackers targeting small firms (Symantec 2015).

1.1.2 Online banking

Since the late 1990s, the financial landscape has changed significantly thanks to the internet (Gkoutzinis 2006). Before online banking, there was distance banking or telephone banking, through which financial services were offered over telephone systems. Financial services are comprised of the full range of functions performed by financial institutions, including, but not limited to, lending, payment services, financial advice, application for products, and inter-account transfers. The provision of ebanking entails "*banking services and the initiation and performance of payments through the banking system by electronic means and other advanced technologies*" (Gkoutzinis 2006). This, therefore, means that internet banking or online banking is the provision of ebanking services over a computer network, such as the internet, through a computer or other access device with internet capabilities (Gkoutzinis 2006).

The researcher uses the term 'online banking' throughout the thesis to refer to any form of electronic or internet banking. Online banking can be provided through a plethora of devices. Apart from personal computers, online banking can be accessed through mobile phones and tablets, giving rise to mobile banking (mbanking). Mbanking is a service that enables users to access banking services through mobile devices (such as a mobile phone or tablet) to conduct banking transactions (Shaikh & Karjaluoto 2015, Alafeef, Singh & Ahmad 2011). Essentially, mbanking is a subset of online banking, as some services are unavailable on mbanking platforms. In the context of this study, online banking encompasses aspects of both mbanking and online banking.

Online banking involves the creation of a login profile. Like any other online profile, the user is required to supply some kind of personal identification information such as bank account details. Given the sensitive nature of online banking, users usually need to visit a branch for verification before their profile is activated. This is important to avoid profile activation based on pseudo-identity, as scammers can create a profile based on credentials obtained through identity theft. The range of value-added services provided varies significantly from one bank to another. Banks usually enter into agreements with other organisations to provide additional services to their clients, such as paying traffic fines, buying electricity, and playing the national lottery through online banking profiles. Given the wide range of transactions that can be performed through online banking, the security of online banking needs to be effective.

From the point of view of the banks, InfoSec of online banking services is vital to limit liability for possible security breaches and to be compliant with the legislation that governs the industry. Sadly, this means that the usability of the service and user experience (UX) come second. In addition, owing to the immaturity of some of the legal frameworks that govern online transactions in South Africa, loopholes are often exploited to circumvent liability for online fraud. This is exacerbated by the spreading of lucrative global cybercrime operated by organised crime syndicates, which is estimated to be beyond a trillion dollars (Grabosky 2014). One way to mitigate InfoSec attacks is to develop online applications that are both secure and usable. This is by no means the ultimate solution to eliminating cybercrime, but it goes a long way in making sure that users use protection mechanisms effectively, without exposing themselves to cyberattacks.

The choice of online banking as case study for this research was motivated by two factors. Firstly, the service fits into the ‘sensitive online application’ domain, as it involves the storage and transmission of financial and personal information of users over the internet. Secondly, security has been identified as one of the obstacles to the adoption of online applications such as online banking and ecommerce. As such, the low adoption of online banking prompted the researcher to investigate the link between the security and usability of the service in the context of usable security.

1.1.3 Usable security design

Interactive design and user-centred design approaches are mainly concerned with developing systems that are usable. Interaction design is about “*designing interactive products to support people in their everyday and working lives*” (Preece, Rogers & Sharp 2015). However, since InfoSec and ease of use are often traded off against each other, the complexity and overheads of InfoSec solutions are often obstacles to their effective and efficient deployment (Dourish & Redmiles 2002). In addition, despite technological advances that have created impressive technical security systems (Choo 2011b), technology does not solve all the InfoSec problems (Schneier 2000). Achieving this balance is a challenge, and while extensive research has been conducted on the technical aspects of InfoSec and usable security principles, there is little research on how to apply these design principles in practice to bridge the gap between theory and practice. Among the more prominent works are the guidelines proposed by Yeratziotis, Pottas, and Van Greunen (2012), Yee (2004b), and Johnston, Eloff, and Labuschagne (2003).

Preece et al. (2015) also outline ways of involving users in the design and development process of products/artefacts through user-centred design. The user-centred design concept has been around since the 1990s, but how to achieve it has not been clear to many designers (Endsley & Jones 2011). Preece et al. (2015) identify three key principles to be used for user-centred design, namely, (1) organise technology around the user's goals, tasks, and abilities, (2) technology should be organised around the way users process information and make decisions, and (3) technology must keep the user in control and aware of the state of the system.

User-centred and interaction design approaches are mainly concerned with developing products that are usable, meaning easy to learn, effective to use, and an enjoyable UX (Preece et al. 2015). Traditionally, usability was associated with learnability, efficiency, memorability, errors, and satisfaction (Nielsen 2010). Apart from usability goals, researchers and practitioners are now looking at improving interaction design systems to cater for additional goals such as UX. Preece et al. (2015) identify a number of UX goals such as being fun, entertaining, and helpful, to name but a few.

Design principles used in practice are commonly referred to as heuristics, which need to be understood in the context of system design by drawing on experience (Preece et al. 2015). An example of a heuristic is how to design a feedback tool, this being quite general and applicable to a wide range of systems. Usability principles (also known as usability guidelines) are more prescriptive by going further, suggesting exactly how to implement design principles (Preece et al. 2015). For example, "*always place the quit or exit button at the bottom of the first menu list in an application*" (Preece et al. 2015). This is a usability principle that specifically tells the designer how to design a system. In addition, whereas design principles, on the one hand, tend to be used mainly for informing a design, usability principles, on the other hand, provide the framework for heuristic evaluation, as they provide more detail to evaluate the usability score of a system (Preece et al. 2015). The need to address not only functional aspects of InfoSec systems, but also system usability, effectively makes such systems socio-technical systems (STS).

1.1.4 Socio-technical systems theory

The importance of designing information systems (ISs) with a view to assisting users to achieve their efficient and effective use dates back to the late 1970s. Bostrom and Heinen (1977) developed the STS theory illustrated in Figure 1-2. The theory describes an IS as comprised of two components, namely, a social sub-system and a technical sub-system, which are independent, but interactive.

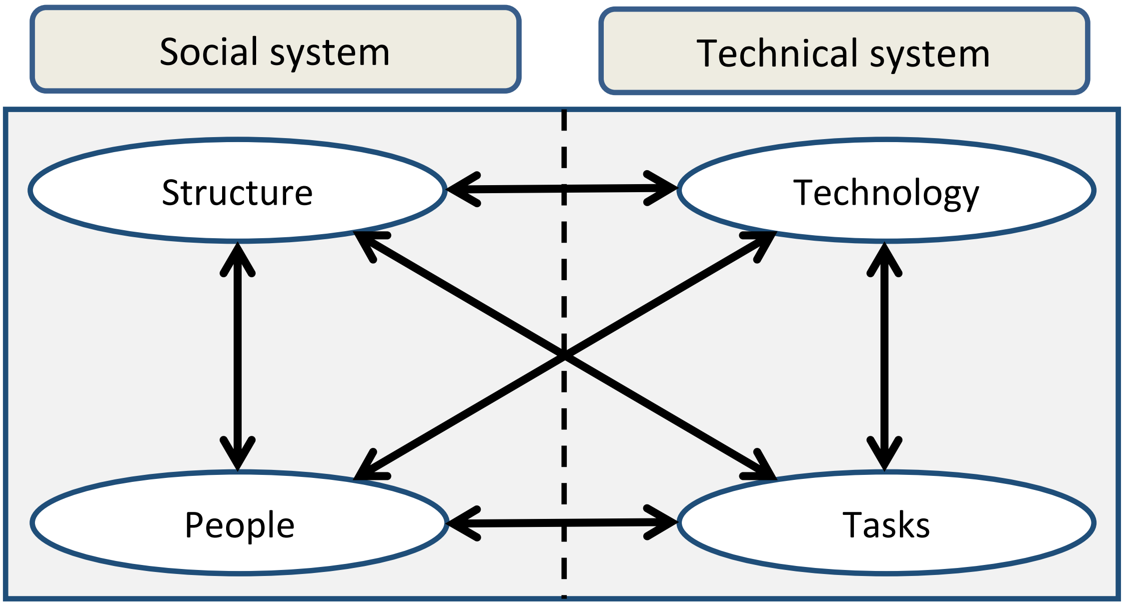


Figure 1-2: Socio-technical system components (Bostrom & Heinen 1977)

The social system is concerned with the attributes of people, while the technical system consists of processes, tasks, and technology needed to transform inputs into outputs. The consideration of usability principles in designing information systems is essentially a way of incorporating socio-technical aspects (Baxter & Sommerville 2011). Online InfoSec systems fit perfectly into this socio-technical definition; hence, their design can be improved by applying this approach. This prompts designers to find a balance between security and usability to allow ISs, especially InfoSec systems, to be used effectively and efficiently by end-users.

1.1.5 Heuristic evaluation

There are a number of usability inspection methods, which include cognitive walkthroughs, formal usability inspections, pluralistic walk-throughs, feature inspection, consistency inspection, standards inspection, and heuristic evaluation (Nielsen 1994c). These methods can be used to evaluate proposed usability design principles. The suitability of each methods depends on the system under investigation and decisions by the system designers. The current research used heuristic evaluation to validate the proposed STInfoSec framework.

The Oxford Dictionary (2018) defines heuristic in computing terms as "*finding a solution by trial and error or by rules that are only loosely defined*", with evaluation defined as "*the making of a judgement about the amount, number, or value of something; assessment*". Heuristic evaluation is a usability inspection method that investigates the compliance of interface features with reputable usability principles (Nielsen 1994b). Evaluation is "*the making of a judgement about the amount, number, or value of something; assessment*" (Oxford Dictionary 2018).

Heuristic evaluation and the use of checklists are closely linked approaches, through which an expert rates the usability of the product on a number of criteria (Lehto & Landry 2012). The first step in a heuristic evaluation is to identify a set of usable security guidelines considered most important for the evaluated product or service. A small number of usability experts (usually five) then use the guidelines to identify usability issues (Nielsen 1994a). Heuristic evaluation is a cost-effective way compared to other usability testing techniques (Nielsen 1994b). The current research involved developing a framework evaluation tool for the design of a secure and usable InfoSec system based on the literature review and findings from the quantitative and qualitative data analyses. The framework was evaluated using the heuristic evaluation method, which allows field experts to evaluate design principles based on checklist items.

1.2 PROBLEM STATEMENT

InfoSec inevitably involves human users for the successful achievement of its intended goals, making its success or failure dependent on how the users use the InfoSec mechanisms designed to protect InfoSec assets. There is an armoury of technical solutions to protect information assets against various attacks, such as properly configured firewalls, antivirus software, and intrusion detection systems. These solutions, on their own, look insurmountable from the perspective of outside attacks, and attackers have acknowledged this fact. Attackers have, therefore, started targeting the generally accepted weakest link in the security chain: the user. Researchers and practitioners agree that InfoSec systems can be better protected through improved design practices.

Given the above assertions, it is clear that an information system that addresses both InfoSec and usability aspects is essentially a socio-technical system that requires an interdisciplinary approach. In 2009, the US Department of Homeland Security listed usable security as one of the 11 most difficult problems to solve in the cybersecurity field (Maughan 2009). Eight years later (2017), that sentiment still holds true, with no clearly defined solution. Although a large body of knowledge has been developed since, usable security remains a challenge, especially with the ever-changing cybersecurity landscape. Hence, in addition to general usable security research, researchers have turned to tackling the problem as it applies to specific applications/information systems.

Green and Smith (2016) argue that not all security problems are caused by end-users, as developers also make mistakes in application development. Hence, the authors call for developer-friendly tools for a holistic solution to application development. The authors, furthermore, argue that security mechanisms are often too complicated, time-consuming, and error-prone for end-users. This has prompted the emergence of the field of '*usable security*'. Researchers in this field attempt to combat user problems with regard to information security through interdisciplinary research to create security mechanisms that are compatible with ordinary users (Green & Smith 2016).

To this end, security and usability have long been considered trade-off aspects in most authentication systems (Van Hamme, Rimmer, Preuveneers, Joosen, Mustafa, Abidin & Rúa 2017, Shay, Komanduri, Durity, Huh, Mazurek, Segreti, Ur, Bauer, Christin & Cranor 2014, Braz, Seffah & M'Raihi 2007, Cranor & Garfinkel 2005). This is highlighted by the fact that, as security increases (for example, long and complex passwords), usability aspects such as memorability and learnability suffer, resulting in users' insecure behaviour, for example, writing down passwords. Information security and computer security have focused mainly on technological solutions to prevent vulnerabilities, while neglecting a socio-technical approach that addresses social aspects from the human side of information security (Kraemer, Carayon & Clem 2009).

There is consensus that systems that are not usable cannot be secure when deployed in the real world (Garfinkel & Lipford 2014). Although the need to address socio-technical aspects in InfoSec has been recognised by practitioners and researchers, the task of developing usable security is proving to be challenging (Cranor & Garfinkel 2005). This phenomenon is not limited to usable security, but also involves InfoSec in general. One aspect identified in achieving usable security is the conversion of theory to practice. There are numerous studies of different aspects of usable security. Besides the challenges of designing usable security, a second dimension of difficulty is the challenge of applying research results in practice (Theofanos & Pfleeger 2011).

Aligning the often-opposing goals of InfoSec and usability has been a challenge so far. This has become a focal area of research with the introduction of the term ‘usable security’, which essentially strives to find ways of developing systems that meet both InfoSec and usability goals. However, while there are several gaps in the knowledge of designing usable security systems, there is extensive research in the separate fields of information security and usability. Currently, there is no agreement on exactly how to design usable security. Scholars have proposed a number of different methods for achieving usable security.

Given that most online applications, such as online banking, are meant for a variety of users with diverse computing skills and InfoSec awareness levels, it is imperative that the design of these systems must address both social and technical aspects. As researchers believe that the application of user-centred design can mitigate online security threats, there is an obvious need for these approaches in developing online InfoSec applications. The problem addressed in this research is that **sensitive online applications do not meet both InfoSec and usability objectives**.

In the context of this research, the term ‘sensitive online applications’ refers to online InfoSec applications that involve the storage or transmission of sensitive and confidential personal information over the internet. Therefore, the applications require effective information security mechanisms for users to use them. This research proposes a socio-technical framework that aims to bridge the gap between theory and practice in developing applications that are both secure and usable.

These applications rely on InfoSec mechanisms to protect sensitive and confidential personal information of users in providing the relevant functionalities. Undoubtedly, all online IS applications require InfoSec mechanisms, but those within the scope of this study deal with critical personal information of end-users. Examples of these applications include online banking, ehealth, and online shopping, to mention but a few. The research proposed a framework to help in the development of secure and usable online InfoSec applications in the context of online banking service.

The framework attempts to provide a solution to fill the gap that still exists between InfoSec solutions and the effective use of these solutions for a secure online environment. Studies on usable security have proposed giving users tools to protect their information such as domain highlighting in browsers (Xiong, Proctor, Yang & Li 2017), strong password guidelines, browser technology, and encryption applications. However, given the diverse skills of online users, it is critical to develop applications with usability considerations built in. Generally, users ignore warnings, not because they intend to be negligent, but due to human habitual behaviour (Anderson, Vance, Kirwan, Jenkins & Eargle 2016). Alsharnouby, Alaca, and Chiasson (2015) found that phishing still worked because users ignored toolbar warnings about phishing threats. As a result, expecting users to act for effective protection against online threats is generally ineffective. The provision of tools without regard for how usable an average user will find them will not improve the InfoSec environment.

1.3 RESEARCH QUESTIONS AND OBJECTIVES

This section provides the research questions guiding the research and outlines the research objectives attained by the end of the research.

1.3.1 Primary research question

The main research question of this study addressed the usability of online InfoSec applications, using online banking as a case study. The main research question was formulated as follows:

> **How can information security-sensitive online applications be designed to be both secure and usable?**

1.3.2 Research sub-questions

The main research question was answered by addressing the following sub-questions:

1. What are the requirements for a socio-technical framework for the development of secure and usable information security online applications?
2. How can a socio-technical framework for the development of secure and usable information security online applications be designed?

3. How can a socio-technical framework for the development of secure and usable information security online applications be validated?

1.3.3 Primary research objective

The main objective of this research is:

> **To develop a socio-technical framework that assists in the development of secure and usable information security-sensitive online applications.**

1.3.4 Research sub-objectives

The main objective was achieved by addressing the following specific objectives:

1. To identify the requirements for a socio-technical framework for the development of secure and usable information security online applications.
2. To design a socio-technical framework for the development of secure and usable information security online applications.
3. To validate the socio-technical framework for the development of secure and usable information security online applications.

The research aimed to develop a socio-technical framework that assist in the development of secure and usable sensitive online applications using online banking as a case study to address both the technical and social aspects of an online environment. The developed framework can be applied to other online InfoSec applications that have similar characteristics as online banking.

1.4 THEORETICAL FRAMEWORK

User behaviour and acceptance of technology in information systems have been explained by a number of theories in the literature, from adoption to acceptance and continued use. The most popular model to explain user behaviour in the interaction with information systems is the second version of the unified theory of acceptance and use of technology (UTAUT) by Venkatesh, Morris, Davis, and Davis (2003). UTAUT2 by Venkatesh, Thong, and Xu (2012) is an extension of UTAUT and is, currently, the latest model that theorises user behaviour with regard to technology acceptance and continued use. UTAUT unifies eight technology acceptance and user behaviour-related theories. Hence, it covers a wide range of constructs that model user interaction and behaviour with information systems. This research applied UTAUT2 in the context of online banking to evaluate the adoption, acceptance, and continued use of the service and a detailed discussion of the model is provided in Chapter 3. The proposed model has additional moderating factors specific to online banking in the South African context.

1.5 RESEARCH DESIGN AND METHODOLOGY

The main purpose of this research was to develop a socio-technical framework that assist in the development of secure and usable sensitive online applications. The proposed framework brings various InfoSec application design principles, guidelines, and concepts together in a comprehensible framework that could be useful for the development of secure and usable information system security applications. The framework consists of socio-technical issues that need to be addressed in developing secure and usable information system applications, especially those that involve InfoSec mechanisms and user interactions. To achieve this objective, the researcher used an MMR design under the pragmatic research paradigm. This section provides a brief overview of the research design and methodology. A detailed discussion of choices made at every stage of the research design is presented in Chapter 4 based on the 'research onion' by Saunders, Lewis, and Thornhill (2016).

1.5.1 The research process

A research process is a multistage process followed when undertaking a research project. It follows a predetermined number of stages. The stages vary in number and exact name based on a number of aspects, which include the author's preference and the type of research being undertaken. Nonetheless, the stages in scientific academic research usually include articulating a research topic, reviewing the literature, identifying the problem, discussing the research philosophy subscribed to, designing the research, describing the research strategy employed, choosing research instruments, collecting research data, performing data analysis, and reporting on results.

The steps of the research process vary depending on the type of research; for instance, the process followed by scientific research differs from that followed in market research. In addition, although the stages are presented in a linear format, the process is essentially iterative, moving back and forth among all stages during the course of the research. Figure 1-3 illustrates the five phases of the research process for this research, mapping each stage to the respective thesis chapter. The research process was guided by the research questions posed and the research objectives outlined in Chapter 1.

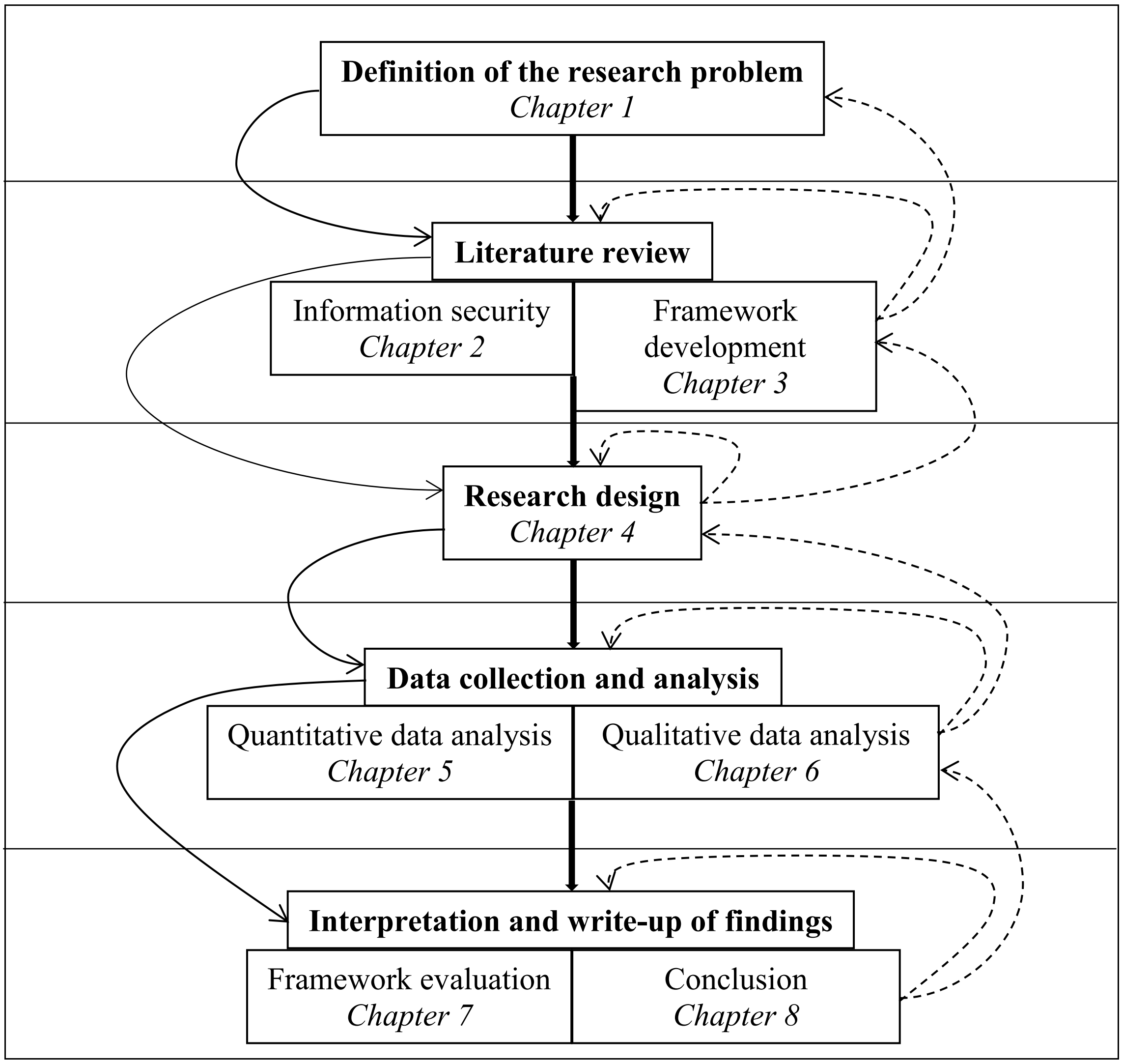


Figure 1-3: The research process

Furthermore, in scientific research, the process may differ based on whether the research is exploratory, explanatory, descriptive, or evaluation research. The rest of this chapter expands on the research design, highlighting decisions made in selecting research options at every stage.

1.5.2 Research design

There are mainly two major philosophical worldviews: interpretive and positivist. Denzin and Lincoln (2017:15) state that, with positivism, *"objective accounts of the real world can be given*". Positivist researchers assume that reality is objective and can be measured with properties that are independent of the researcher and instruments used (Myers 2013).

Positivism is mainly associated with quantitative research that focuses on collecting quantitative data for theory testing. The interpretive paradigm is primarily associated with qualitative research designs. It is also worth noting that both (positivism and interpretive) paradigms can be applied in quantitative or qualitative research, based on the way the researcher chooses to frame the study. Among the other paradigms besides positivism and interpretivism are social constructivism, postpositivism, critical realism, and pragmatism, to mention but a few.

Pragmatism, the paradigm used for this research, is located in the middle between the opposing forces of positivism and interpretivism, giving the researcher the freedom to use aspects of both quantitative and qualitative research methods (Creswell & Clark 2017, Doyle, Brady & Byrne 2009). Pragmatism acknowledges philosophical assumptions of both positivism and interpretivism, such as the existence of a single objective reality and that reality consists of subjective views wedged in the mind, respectively (Creswell & Poth 2017). The pragmatic philosophy asserts that human action cannot be separated from past experiences and behaviour that has arisen from those experiences; hence, the meaning of actions and beliefs is found in their consequences (Levin & Greenwood 2013). Morgan (2014) succinctly summarises the relevance of pragmatism by stating that individuals will have different worldviews because no two previous experiences can truly be identical; as such, worldviews are both individually unique at the most detailed level and socially shared at broader levels.

This research followed a mixed methods research (MMR) design, making pragmatism the paradigm of choice. The paradigm used here acknowledges the philosophical assumptions of both the positivist and interpretivist paradigms and, thus, asserts that human action cannot be separated from experiences and behaviour arising from those experiences; hence, the meaning of actions and beliefs is found in their consequences (Levin & Greenwood 2013). In other words, reality is discovered through abduction, which is "*uncovering and relying on the best of a set of explanations for understanding one's results*" (Johnson & Onwuegbuzie 2004:17). The researcher argued that the intersection of human behaviour and InfoSec, commonly referred to as 'usable security', which was the subject of this research, was an area that was not straightforward and that conventional solutions had failed to provide effective solutions. Therefore, applying a pragmatic philosophy that did not view the world through a single lens was likely to contribute significantly to, firstly, understanding the problem and, secondly, proposing solutions.

1.5.3 Research methodology

The research methodology outlines all aspects of research project implementation, guided by the research design. Research methodology is a part of the overall research design that concentrates on the intrinsic details of gathering research evidence, that is, aspects with regard to data collection and analysis. The researcher used an abductive approach, as this fitted in with the pragmatic mixed research design that involved testing an extant theory and establishing an explanation for InfoSec user behaviour. The research collected survey data to explain online banking adoption and continued use, while investigating design principles that might assist in developing a service that met both security and usability goals. This formed the deductive part of the abductive approach, while qualitative interviews of system designers inductively investigated perceptions of user behaviour in system development and maintenance.

1.5.4 Mixed methods research design

There is an ongoing debate on different stances that ought to be taken in MMR designs. Creswell (2010) and Greene and Hall (2010) note the resistance to mixing paradigms based on the argument that paradigms are unique and cannot be combined in a single research project. Denzin and Lincoln (2013) contend that paradigms are independent and can be combined into achieving the objectives of a single research project. In addition, Mingers (2001) argues that research methods can be separated from paradigms and can be used critically and knowledgeably to address social problems that are laden with societal and individual self-understandings. This debate leads Creswell (2010) to acknowledge the differences in paradigms – hence, the need to keep them separate in MMR designs. This essentially implies the use of two paradigms in MMR. Given these disparate views, the discussion of MMR paradigms continues. The researcher subscribed to the notion of applying two paradigms (interpretivism and positivism) in a pragmatic study. Creswell and Clark (2017:5) define MMR as follows:

> "*As a methodology, it involves philosophical assumptions that guide the direction of the collection and analysis and the mixture of qualitative and quantitative approaches in many phases of the research process. As a method, it focuses on*

collecting, analysing, and mixing both quantitative and qualitative data in a single study or series of studies."

The researcher used MMR for *additional coverage* that sought to assign different strengths of different methods to different goals of the research project (Morgan 2014). This approach was used through the *convergent parallel mixed methods design*, as illustrated in Figure 1-4.

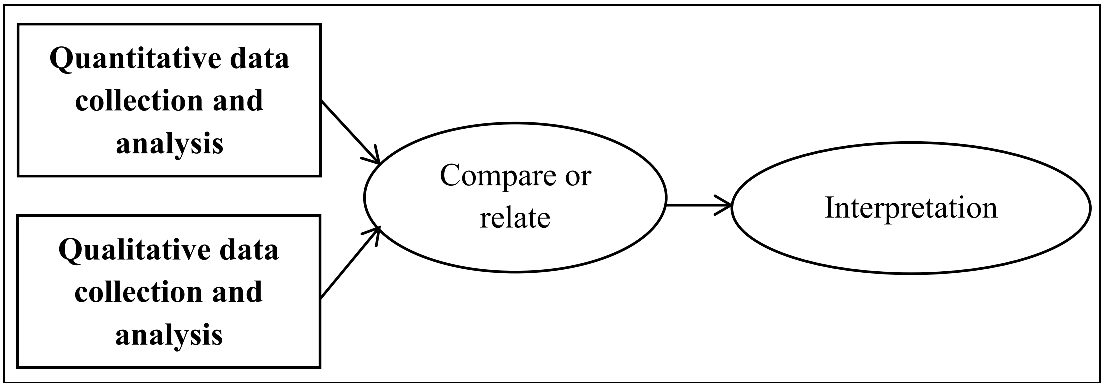

Quantitative data collection and analysis
Qualitative data collection and analysis
Compare or relate
Interpretation

Figure 1-4: Convergent parallel design (Creswell & Clark 2017)

The researcher independently implemented both the quantitative and qualitative strands, with separate analysis, before combining the findings in a final interpretation. The final interpretation fed into the proposed research framework for the development of secure and usable online InfoSec applications. The framework was evaluated through a heuristic evaluation method.

1.6 ETHICAL CONSIDERATIONS

The research was reviewed and approved by the Research Ethics Committee of the College of Science, Engineering, and Technology, Unisa. A written approval certificate was issued to the researcher that was made available to both research participants and respondents. The ethical clearance certificate was included in the documentation package containing the invitation to participate, while the certificate was made available to survey respondents on request. The ethical certificates are included as Appendix A.

The research participants and respondents were given informed consent forms explaining the research and their respective participation. These forms included the contact details of the researcher, the supervisors, the research ethics chairperson, and the university's toll-free hotline to allow research participants and respondents to report any unethical behaviour. The ‘letter of informed consent’ and ‘participant’s information sheet’ for survey respondents, interview participants, and framework evaluators are included as Appendix B, Appendix C, and Appendix D, respectively. The researcher also applied for permission to invite Unisa staff and students to participate as survey respondents. Unisa’s approval to conduct research involving Unisa staff and students is included as part of the ethical certificates in Appendix A.

1.7 RESEARCH PURPOSE AND CONTRIBUTIONS

The purpose of this research was to examine social and technical aspects that could assist in the design of online security systems and to propose a usable security framework to assist in addressing socio-technical aspects in the design of online InfoSec applications. The research aimed to make the following contributions to the fields of ISs and usable security:

- Contribute to the field of usable security by proposing a framework for designing usable security that addresses socio-technical aspects.
- Develop a usable security framework evaluation tool for the assessment of an online InfoSec application website.
- Provide new insights into the use of an MMR design in information systems.
- Make a practical contribution to the envisaged improvement in the user-centred design and development of online banking websites. This would help make the wider ecommerce environment more secure.

1.8 RESEARCH SCOPE

The intention of the research was to investigate the acceptance of online banking and evaluate the usability of online banking security websites based on relevant data gathered from the users of major banks in South Africa. A framework for the design of usable security of online InfoSec applications was proposed. The proposed framework was evaluated by means of a heuristic evaluation method using a checklist of items based on identified usable security principles.

1.9 LIMITATIONS

The research used online banking as a case study for the development of usable security of online applications. Hence, the application of the proposed framework to similar online applications might need small adaptations, depending on how similar or dissimilar the application environment is from the case study used. The researcher envisaged that the findings of this research would provide fundamental building blocks to provide solutions to similar problems in a different environment.

The research investigated barriers to the adoption and continued use of online banking based on the perceptions of users who were currently using the service. Although these users could help highlight factors that made users hesitant to take up the service, a more in-depth investigation of adoption problems can be achieved by obtaining the perceptions of users not yet using the service.

The proposed framework was not intended to solve problems associated with user behaviour regarding InfoSec, but was meant to complement current proposed solutions in the field by contributing to the body of knowledge. Hence, even its implementation would need to take other aspects into consideration that might come from other fields and research studies and ought not to be done in isolation. The InfoSec problem is now considered a social problem, with many facets that require a holistic socio-technical approach to finding solutions. This holistic view requires the input of all stakeholders in the environment where information systems are developed and deployed, with emphasis on a user-centred approach. The government needs to play a central role in educating citizens (especially at an early age) regarding the threats to InfoSec in a digital economy.

1.10 THESIS STRUCTURE

The research roadmap presented at the beginning of each chapter was based on the five stages of the research process, as illustrated in Figure 1-5. The research roadmap illustrates the position of each of the eight chapters of the thesis. The left-most column indicates the stage in the research process, accompanied by the chapter(s) in each stage to its right. The position of each chapter on the roadmap is in bold and highlighted with a darker shade. The roadmap is presented at the beginning of each chapter. The following is a synopsis of the content covered in each of the eight chapters of the thesis.

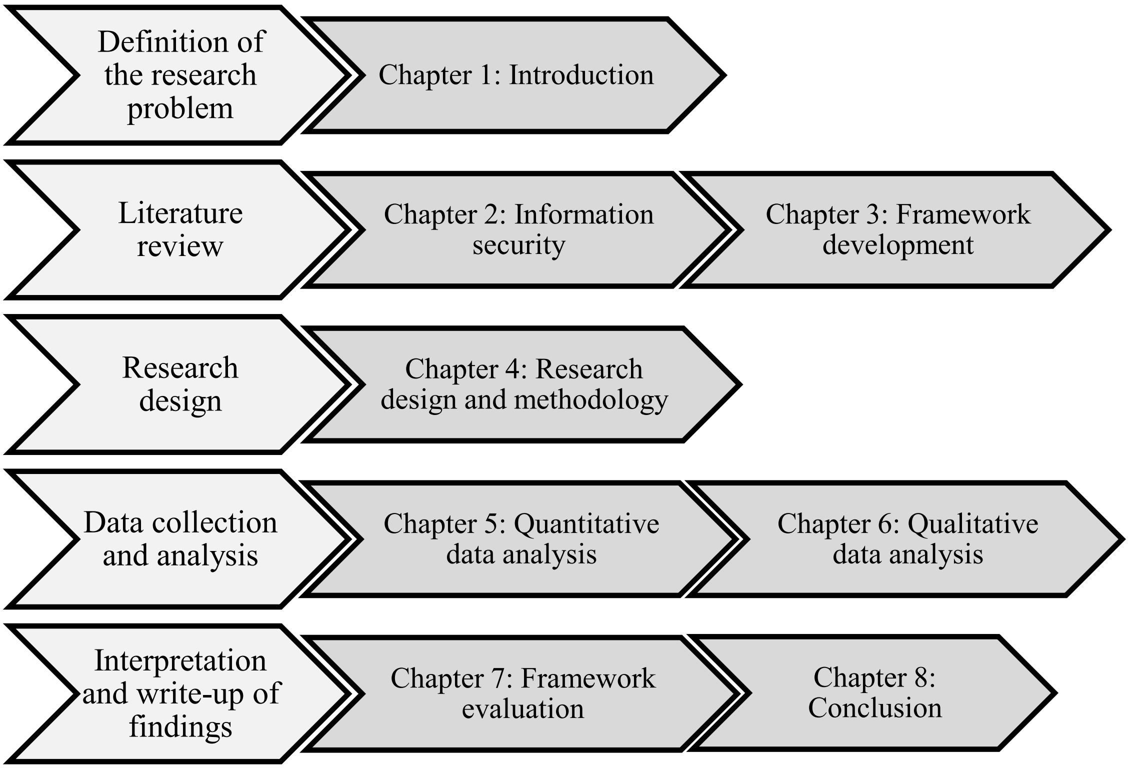

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 1-5: The research roadmap

Chapter 1: Introduction

The chapter defines the scope of the research by first giving the background, which then builds up to the problem statement. This is followed by the presentation of the research questions and research objectives, which guide all the other activities and decisions made in addressing the problem area. A brief introduction to the theoretical framework that guides the research is given, followed by a brief discussion of the research design and methodology. Lastly, the chapter concludes with ethical considerations, research contribution, and limitations.

Chapter 2: Information security

The literature review is presented in two chapters. The first of these chapters briefly touches on the topics of the internet and ecommerce, as online banking is provided through the internet and an integral part of the ecommerce payment system. This is followed by a detailed discussion of InfoSec, which includes the fundamental principles, InfoSec threats, online InfoSec, and – lastly – threats to online banking security.

Chapter 3: Framework development

This second literature review chapter discusses details of human-computer interaction (HCI) and usability, with emphasis on how these are linked to the focus of the research:

usable security. The chapter also presents usable security as a socio-technical system, as it relates to both technology and human aspects. This is followed by usability and UX goals, user-centred interaction design, and website usability. Finally, the chapter presents the preliminary STInfoSec framework, for whose validation the research collected data.

Chapter 4: Research design and methodology

The chapter outlines the overall blueprint of the research project, giving details of the selected research design and methodology, including motivations for each selection. The chapter provides detailed discussions of, and motivations for, the following research choices: the research paradigm (pragmatism), the research process, the research approach (abductive), research strategies (survey and case study), and data collection and analysis techniques.

Chapter 5: Quantitative data analysis

The process of the quantitative data collection and analysis of the MMR design is presented in this chapter. The chapter starts with an outline of the theoretical framework guiding data collection and research hypotheses, followed by details of data collection techniques used. This is followed by a brief discussion of the data analysis techniques used and how these were applied in the research. The analysis included descriptive and inferential statistics. Structural equation modelling was used for inferential statistics, and this is presented together with the respective measurement models. Finally, the model is interpreted and linked to the research objectives.

Chapter 6: Qualitative data analysis

The qualitative part of the research is presented in this qualitative data collection and analysis chapter. The chapter starts by discussing the sources of data, namely, interviews and qualitative survey responses. This is followed by a detailed discussion and application of the data analysis method used in the research, that is, framework analysis. The stages of framework analysis are outlined, followed by the final stage, which summarises the mapping and interpretation of the qualitative findings, linking them to the overall objectives of the research project. The chapter concludes with a presentation of six themes identified based on thematic and open coding, using an *in vivo* coding technique on participants' responses and, finally, linking them to the usable security principles that formed the preliminary socio-technical information security (STInfoSec) framework, for evaluation in Chapter 7.

Chapter 7: Framework evaluation

The main objective of the preceding chapters was to develop a socio-technical framework. The objective of this chapter is to present the framework and conduct an evaluation. The chapter first presents the integration of quantitative and qualitative findings, highlighting how these support the proposed preliminary STInfoSec framework. The preliminary framework is presented, followed by the evaluation process carried out through heuristic evaluation by field experts in the areas of security and usability. Finally, the validated STInfoSec framework is presented.

Chapter 8: Conclusion

The final chapter concludes the research project by first discussing how the research questions were answered and research objectives achieved after conclusion of the research project. This is followed by a discussion of the research contribution both in theory and in practical terms. Limitations of the study are provided, followed by suggestions for further work. Lastly, a summary that provides the researcher's reflections is given.

1.11 CHAPTER CONCLUSION

Chapter 1 pointed out the research gap and outlined the problem statement, including stating research questions and objectives. The challenge in designing usable security is finding a balance between information security and usability needs. The use of design principles has been identified as one potential solution to achieve usable security. Several design principles are proposed in the literature; however, the challenge is that such principles are generalised, while there is a need for specific design principles for applications. This research proposes a design framework for sensitive online applications, using a socio-technical approach, validated specifically for online banking service. Chapter 2 outlines the information security needs of online applications; hence, it focuses on the technical component of the socio-technical approach of this research.

-- oOo --

CHAPTER 2 LITERATURE REVIEW

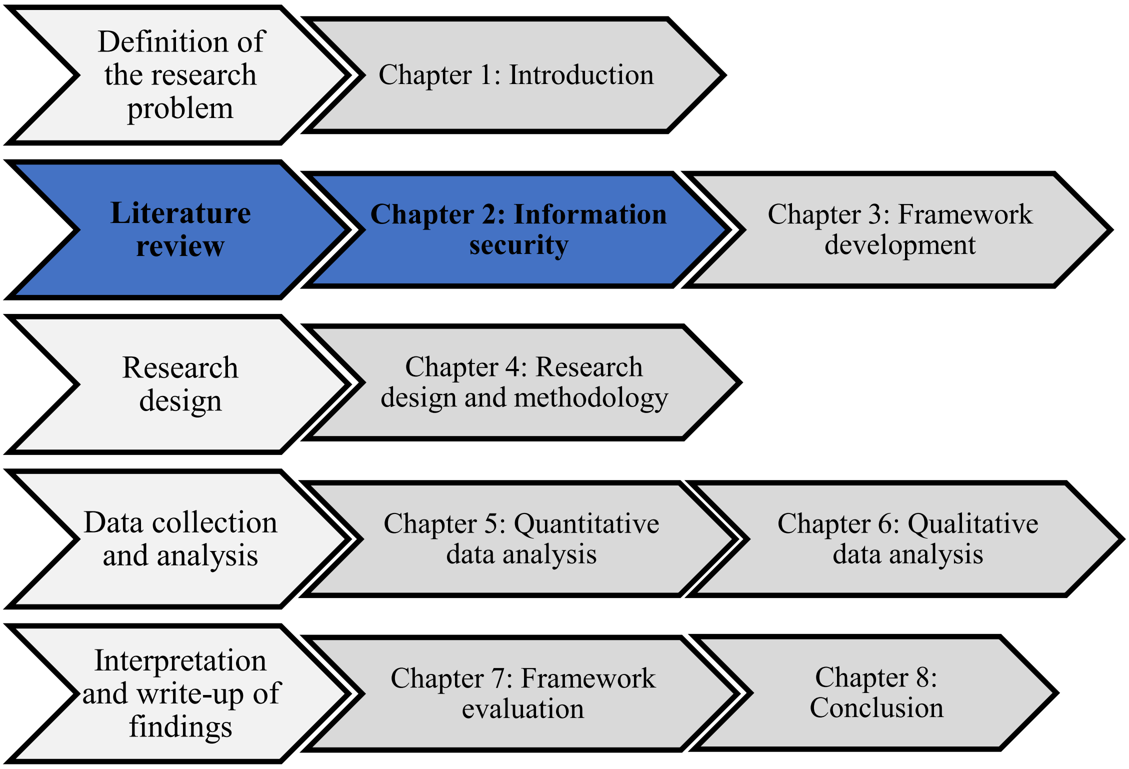

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 2-1: The research roadmap

2.1 INTRODUCTION

Since its development, the internet has evolved, and it has advanced to such an extent that it has changed the way people carry out their daily activities. Almost any activity can be performed online, from communication and entertainment to buying and selling products and services. Organisations and governments hire, train, and pay their employees online. The advent of ecommerce, which relies on the internet, has revolutionised individuals' lifestyles and the business processes of organisations. The migration of business processes to online platforms has drastically reduced the operating costs of organisations (Hernando & Nieto 2007). Hence, most organisations encourage their clientele to use online channels rather than brick-and-mortar channels, thereby cutting down on the operational costs of these brick-and-mortar locations. For financial institutions, the move allows for a reduction in behind-the-desk employees to service walk-in clients at branches. Banks now offer a free online banking service to encourage the adoption of the service, but, in spite of the obvious benefits of ecommerce and related services, the uptake of the service is still lacking, especially in developing economies (Statista 2012).

2.2 INTERNET

Online ISs rely on the internet to remotely access data through a plethora of connected end-user devices. The internet is a public network that connects billions of computing devices and networks of different sizes globally, giving internet access to billions of users (Bidgoli 2006). The internet has revolutionised modern society, as described by Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, and Wolff (2009:22):

> "*The internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location*."

With the internet as a medium for information dissemination, organisations and individuals are becoming progressively more reliant on the internet's 24/7 connectivity for access to, and distribution of, information. Unfortunately, the internet was not built with security as an integral component. Oppliger (1997:92) describes the beginning of the internet as:

> "[a] *collegial environment, where the users and hosts were mutually trusting and interested in a free and open exchange of information. In this environment, the people on the internet were the people who actually built the internet*".

Today, the internet environment is expansive with potentially adversary nodes that are untrustworthy. At the time of writing this thesis, there were over 3.83 billion internet users and even more devices connected to the internet, transmitting over a billion gigabytes of data a day (Internet Live Stats 2018). Given these figures, it is inevitable that a number of online users will be novices with little or no basic InfoSec awareness – hence, the need to address the InfoSec problem to protect sensitive and confidential information, as it is stored on devices and transmitted over the internet. In a layered InfoSec approach, different aspects of InfoSec are addressed at different layers. Usable security, the focus of this research, is essentially situated at the topmost layer.

The web browser is still the primary means of accessing internet content from desktop and portable (laptop) computers. However, the introduction of smartphones has brought about a variety of applications that provide internet content directly without the use of the web browser. Such applications need to be developed with InfoSec intrinsically included without relying on web browser security. The web browser is also used in mobile devices such as smartphones for internet access, bringing the internet to the fingertips of users, regardless of computer-proficiency levels. However, being an open and public medium, the internet brings with it new risks and threats to the confidentiality, integrity, and availability of information. Web browser security mechanisms such as the HTTP over TLS (HTTPS) protocol can only go so far in protecting users' information, but recent attacks such as phishing bypass these protections and leave users vulnerable to numerous online security threats. Therefore, the search for effective solutions to online InfoSec problems is ongoing. One area that has gained momentum is the development of usable IS applications. This research investigated a framework to promote the development of secure and usable online InfoSec applications, using online banking as a case study. Online banking is a major component of electronic commerce, as it forms part of the payment system when products and services are sold online.

2.3 ELECTRONIC COMMERCE

Electronic commerce (ecommerce) is the buying, selling, transferring, or exchanging of products, services, and/or information via a computer network, including the internet (Turban et al. 2015). Ecommerce has evolved from just the selling and buying of products and services to involving servicing customers and collaboration among business partners. Therefore, the term 'electronic business' (ebusiness) has been coined to sufficiently cover broader aspects of ecommerce, essentially making ecommerce a subset of ebusiness (Turban et al. 2015). Turban et al. (2015) define ebusiness as an extension of ecommerce in that it goes beyond the selling of products and services online and also includes conducting business processes online such as communications, customer services, and marketing.

Significantly, as mentioned before, ecommerce has revolutionised the way organisations and governments do business and how individuals perform their day-to-day lifestyle activities. However, with the widespread adoption of ecommerce, the data transmitted through ecommerce channels include sensitive and confidential information such as personal and financial details. Consequently, with the internet being open, it is important to protect data during transmission and storage against unauthorised access or modification. Ecommerce is a global model, and the sections that follow discuss general ecommerce issues that are prevalent in the majority of economies. Undeniably, certain regions face additional challenges. For example, in developing countries, there is a lack of internet infrastructure, which adversely affects internet speed and cost, resulting in low internet penetration rates (Shiferaw & Zolfo 2012).

Although ecommerce is growing globally, the Information Infrastructure Task Force (IITF) has identified the following key issues that need to be addressed before ecommerce can be fully realised. The issues include security of electronic transactions, interoperation of communications, data management, and security services, plus the identification and removal of economic, cultural, regulatory, and legal barriers (Han & Noh 1999). These barriers are applicable globally, although with varying severity from country to country. In the context of South Africa, the cost of internet connectivity, coupled with lack of internet infrastructure, continues to be a major barrier to ecommerce adoption (Chetty, Banks, Brush, Donner & Grinter 2012). Therefore, a lot of work still needs to be done to improve the speed of broadband connection and reduce internet cost to allow the majority of the population easy access. An improvement in ecommerce adoption will directly influence adoption of other services such as online shopping and online banking, as well as service delivery by government through initiatives such as egovernment. Electronic services such as online banking and online shopping, tend to have common barriers to adoption. One such barrier is InfoSec, which strives to protect personal and confidential information in storage and in transit over an open and public internet connection. This research investigated ways of improving online InfoSec through the design of online applications. The researcher proposes a socio-technical approach that promote effective use of InfoSec mechanisms in online applications, thereby encouraging adoption of these InfoSec sensitive applications.

2.4 INFORMATION SECURITY

There is no doubt that, in this digital world, information is important to individuals and organisations alike. This section defines InfoSec and provide fundamental principles that need to be addressed for effective protection of information assets. The nature of an online environment make InfoSec critical for trust between geographically dispersed and often untrustworthy entities. To address the InfoSec problem, these aspects are applicable to both online and offline environments, but with special emphasis on online InfoSec, the main subject of this research. In business, information can be the difference between achieving business objectives and failing to meet these objectives. It then follows that information is the most important business asset (Peltier, Peltier & Blackley 2005) and that its protection and safeguarding against unauthorised access are important (Thomson

& Von Solms 2005) and essential to maintaining the competitive edge, profitability, cash flow, and reputation of an organisation (Tryfonas 2010).

Security, in general, is concerned with the protection of assets, and one has to know one's assets to be able to protect them (Gollmann 2011). The Oxford Dictionary (2018) defines security as "*the state of being or feeling secure*". The primary objective of security is protection against intentional or unintentional harm. There are multiple layers of security in an organisation. Whitman and Mattord (2017) outline six layers of security, as illustrated in Figure 2-2. For effective protection, each of these layers needs attention, and a weakness in one layer can compromise the whole system.

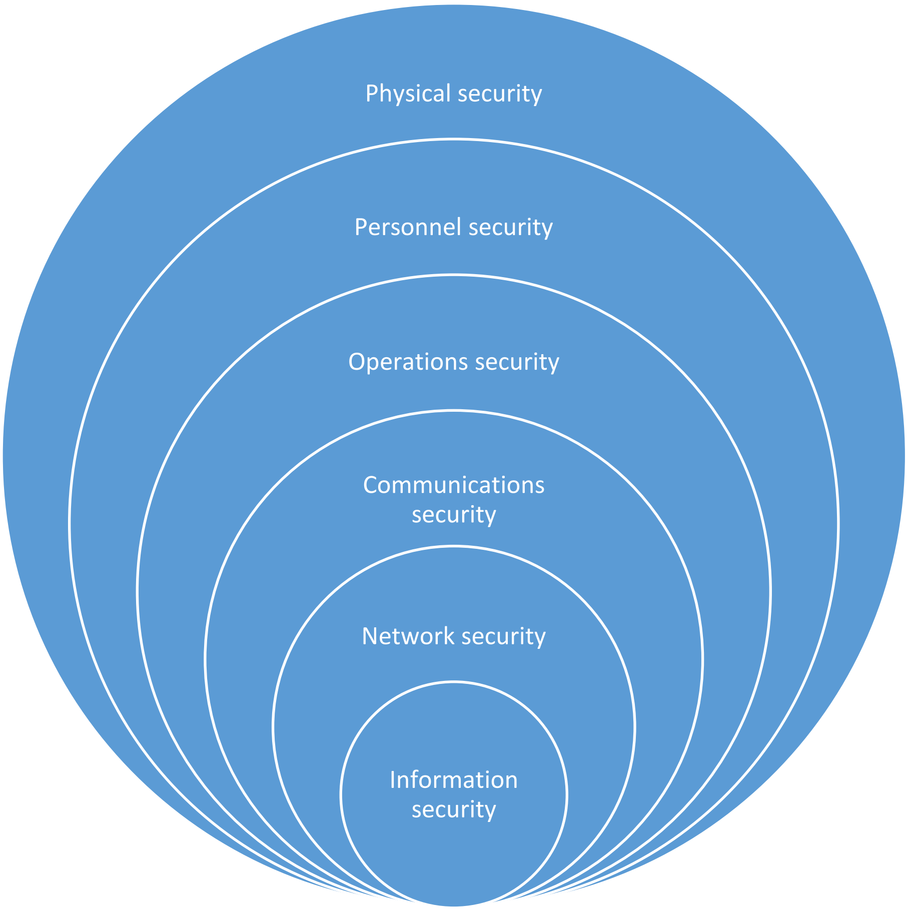


Figure 2-2: Layers of security (Whitman & Mattord 2017)

The first layer, *physical security*, protects physical objects or areas against unauthorised access. *Personnel security* protects the individual or group of individuals authorised to access the organisation and its operations. The next layer, *operations security*, protects the details of a particular operation or series of activities. Communications media, technology, and content are protected through *communications security*. *Network security* protects networking components, connections, and content. Lastly, *information security* protects the confidentiality, integrity, and availability of information assets in storage, processing, or transit.

Computer security is the prevention and detection of unauthorised actions by users of a computer system (Gollmann 2011). Computer security first concentrated on securing data storage before the widespread use of computer networks. It evolved into the securing of data in transmission and the transmission medium itself. Computer security is synonymous with cybersecurity, which Touhill and Touhill (2014:1) define as:

> "[t]*he deliberate synergy of technologies, processes and practices to protect information and the networks, computer systems and appliances and programs used to collect, process, store and transport that information from attack, damage and unauthorised access*".

The term 'information security' has a broader meaning than 'computer security'. There is, however, no consensus on the precise definition of InfoSec, as the definition changes based on the context. Depending on one's viewpoint, there are many definitions of InfoSec, as it can be viewed from a technical, behavioural, managerial, philosophical, or organisational standpoint (Zafar & Clark 2009). A number of different definitions have been advanced by researchers and practitioners. Some of the definitions from varying sources are given below.

Peltier (2014) argues that InfoSec covers a number of aspects, namely, security policy, organisational security, asset classification, personnel security, physical security, access control, communications and operations management, system development and maintenance, disaster management, and – lastly – compliance. This implies that InfoSec is not only concerned with information stored in digital form, but even printed information and tacit knowledge of personnel.

InfoSec is "[t]*he protection of information against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional*" (Blyth & Kovacich 2006:4). According to Peltier (2014), InfoSec consists of using access controls to grant access to information assets and prevent unauthorised access and damage. McDaniel (1994) defines InfoSec as the use of concepts, techniques, and technical and administrative measures to protect information assets against deliberate or unintentional authorised acquisition, damage, disclosure, manipulation, modification, loss, or use.

A recurring phrase in most definitions of InfoSec is ‘information asset’. An information asset is an organisational resource being protected. Assets can be logical, such as data, or physical, such as a computer server (Whitman & Mattord 2017). Many definitions of InfoSec and some definitions of computer security include the principles of the CIA (confidentiality, integrity, and availability) triad as the fundamentals of InfoSec. Anderson (2003) argues that InfoSec cannot be all about CIA due to the lack of agreed meanings of the CIA principles; hence, we need a new definition. Therefore, for InfoSec measures to work, security professionals need to agree on exactly what constitutes InfoSec. One theme found in all definitions is that InfoSec is an all-encompassing concept that can be achieved by subdividing numerous information system concepts and addressing them individually for the protection of the information assets of an organisation (Anderson 2003).

The protection of information against unauthorised access is becoming more important, especially now that many organisations store and transmit personal and confidential data pertaining to individuals. Such data is now stored at remote cloud locations and retrieved through the public and open internet. Given the recent high-profile security and privacy breaches at Yahoo, Target, JPMorgan Chase, Ashley Madison, and eBay (Information is Beautiful 2018), it has become apparent that organisations that collect personal information cannot be left to monitor themselves.

South African organisations are not currently legally compelled to report and make security breaches public, although this might change with the introduction of the Cybercrimes and Cybersecurity Bill, which is in the process of being enacted. A recent disclosure of about 60 million personal records of South African citizens, deemed the largest South African data breach, was attributed to poor information safeguards by a company that holds real estate information (Fraser 2017). It is interesting to note that the breach was not a hack, but due to data stored on an unprotected web server easily accessible to anyone. This is a violation of the Protection of Personal Information (PoPI) Act. The recent Equifax data breach in the USA was due to the delayed application of a fix that could have avoided the breach (Newman 2017). Hence, in addition to cybercriminals’ continuous attempts at accessing personal information of citizens, there are still some organisations that are not implementing the most basic protection mechanisms to safeguard personal information. The PoPI Act serves the purpose of ensuring that all South African institutions that collect, process, store, and share another entity's personal information conduct themselves in a responsible manner by holding them accountable (PoPI 2013). However, some international breaches such as those at Yahoo, Ashley Madison, and eBay do have a global impact that affects all individuals, regardless of country of residence.

Governments have enacted data protection laws to give guidelines on what is expected when third parties collect and store personal information. Accidental or fraudulent loss of data can have serious implications for the custodian of information and clients. Personal information collected by organisations and governments ranges from names and addresses to sensitive data such as credit card numbers. A security breach of such information can damage the reputation of the organisation and result in the loss of future business. This can lead to a serious inconvenience for clients, with threats such as identity theft.

If viewed as a social science that examines the behaviour of individuals as they interact with systems, InfoSec begins and ends with the people inside and outside the organisation who interact with the system (Whitman & Mattord 2017). This follows Dhamija and Perrig's (2000) earlier argument that systems should be evaluated not only theoretically, but also by how secure they are in common practice. Parsons et al. (2010) affirm that an exclusive focus on the technical aspects of security is inadequate without due consideration of how the human users interact with the system. Nevertheless, designers do not always take human cognitive limitations into consideration in their design and evaluation of information system security (Dhamija & Perrig 2000).

2.5 PRINCIPLES OF INFORMATION SECURITY

The challenge of providing solutions to the InfoSec problem involves addressing numerous challenges that are interdependent, resulting in a holistic solution. InfoSec in general consists of numerous principles that need attention to achieve effective system security. However, the nature of online applications poses the additional challenge of granting access to remotely connected devices. This section discusses the principles, especially those fundamental to providing InfoSec solutions to ISs that operate in an online environment. Traditionally, there were three main principles of InfoSec, often denoted by the CIA triad (Stamp 2011). Parker (2012) has since argued that the classic CIA triad is inadequate to allow security practitioners to address the InfoSec problem practically, as many aspects are left unaddressed. Hence, Parker (2012) proposes a new framework with additional principles, namely, utility, authenticity, and possession. These principles are interdependent and cannot be addressed in isolation. The following sections discuss the original CIA triad principles and other principles that have emerged as important and that need to be addressed individually in the broader realm of InfoSec. These principles are critical in online InfoSec applications, as a single weakness can compromise the whole system. This section, thus, discusses all the main principles of InfoSec.

2.5.1 Confidentiality

Confidentiality is the assurance that information is not disclosed to inappropriate or unauthorised entities or processes (Whitman & Mattord 2017). Confidentiality ensures that information is accessible only to those authorised to have access. Confidentiality ensures that those allowed to access information are able to, and will be allowed to, manipulate the information based on their rights and privileges. Confidentiality is often referred to as secrecy or privacy. Privacy refers to the protection of personal data, while secrecy refers to the protection of organisational data (Gollmann 2011). In an online environment, this principle is critical to ensure that, as data travels through numerous network nodes, some of which are untrustworthy, it is not intercepted and modified before reaching the final destination.

2.5.2 Integrity

Integrity ensures that information can be modified only by authorised entities in authorised ways, thereby ensuring that it is not accidentally or maliciously altered or destroyed, be it in storage or in transit (Whitman & Mattord 2017; Peltier 2014). Information assets should be modified only by authorised parties and only in authorised ways (Pfleeger & Pfleeger 2015). In security terms, information integrity ensures that information is accurate and has no unauthorised modifications (Graham, Olson & Howard 2011). It is, therefore, important to be able to identify any modifications that might have been applied to the received information during transmission to allow the recipient to discard such information.

2.5.3 Availability

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provide the ISO/IEC 27000:2016 standard, which defines availability as ensuring that authorised entities have access to information and associated assets when needed. This means that one is assured, with reasonable confidence and certainty, that the information and the information systems are always available when needed (Blyth & Kovacich 2006). Availability can mean different things to different people. Generally, a data item, service, or system is available if there is a timeous response and a fair allocation of resources, if the service or system is used easily, and if there is controlled concurrency to support simultaneous access, deadlock management, and exclusive access as required (Pfleeger & Pfleeger 2015).

The main threat to availability is a denial-of-service (DoS) attack, particularly distributed DoS (DDoS) attacks that are prevalent in the current networked online environment. DDoS is the prevention of authorised access to system resources or the delaying of time-critical services, which occurs by inundating web server bandwidth or resources with multiple targeted requests (Zargar, Joshi & Tipper 2013). DDoS attacks are usually carried out through compromised internet nodes, known as ‘zombie computers’; a collection of such interconnected nodes on the internet is called a ‘botnet’ (short for ‘robot network’) (Zargar et al. 2013). One of the main attractions of online services is the convenience of being able to access the services 24/7, which makes availability a principle critical to providing online services to users.

2.5.4 Authenticity

Authenticity means conformance to reality. The authenticity of information generally refers to wholeness, completeness, and good condition (Parker 2012). Authenticity is achieved through the use of authentication mechanisms. Authentication is an access control method that validates a system entity’s claimed identity, before granting permissions and creating an audit trail (Peltier 2014). There are a number of authentication mechanisms for specific applications. For example, computer system users are authenticated through usernames and passwords, and the authenticity of documents can be achieved through digital signatures. In other words, confidentiality ensures that the entity’s identity, when requesting access, is not modified (in storage or in transit) and reflects the entity’s originally claimed identity. Through encryption mechanisms, confidentiality protects the information that uniquely identifies the entity. Authentication plays a significant role in online applications that are intended to be accessible remotely from a multitude of devices. Access devices, web servers, and remote databases that store personal information need to provide infallible authentication mechanisms to authorised users with different access rights.

2.5.5 Non-repudiation

Non-repudiation ensures that an entity or party cannot later deny being the origin of data or communication (Peltier 2014). Non-repudiation can be defined as a property that prevents an entity from denying actions performed on information assets (Pfleeger & Pfleeger 2015). It provides unforgeable evidence that a specific action occurred.

2.5.6 Accuracy

Information accuracy requires that information be free from mistakes or errors and, more importantly, that it has the value that the end-user expects (Whitman & Mattord 2017). For example, financial information such as a bank balance can be accessed at anytime from anywhere using multiple channels. Hence, it is vital that such information is always up to date. Accuracy of information is assured by gathering information from reliable sources and securely keeping the information in an environment where any modifications, authorised or unauthorised, can be identified (Pipkin 2000).

2.5.7 Utility

Parker (2012) describes loss of utility as the loss of usefulness of information that still has confidentiality, integrity, and availability. An example of utility loss is where an encryption key to an encrypted document is permanently lost. The information in the document is still protected against unauthorised access and modification, but is inaccessible to the authorised user. Nielsen (2010) suggests that a product or service first needs to be useful and then provide utility to the user before addressing usability. Therefore, online applications have to provide a utility to the user, and necessary safeguards to protect the utility are important.

2.6 ACCESS CONTROL

Access control is a cornerstone of InfoSec and security, in general, especially since any security violation begins with perpetrators gaining access, be it authorised or unauthorised. Hence, the starting point of any security discussion is access control. Access control approaches rely on a number of InfoSec principles such as identification, authentication, authorisation, and accountability (Whitman & Mattord 2017). Identification verifies the identity of an applicant, while authentication validates the purported identity using authentication mechanisms based on supplied information. There are three main approaches to identification and authentication: 'something you know' (for example, a username and password or personal identification number (PIN)), 'something you have' (for example, an access card), and 'something you are' (for example, a fingerprint). Based on how many of these three elements the system requires, the system is a one-, two-, or three-factor authentication mechanism.

The 'something you know' approach is a single-factor authentication (SFA) mechanism widely used in online systems, where the user accesses the system by supplying a combination of a username and password, previously acquired on registration. This approach is simple, cost-effective to implement, and very convenient for users. System administrators allow users to reset forgotten passwords and request forgotten usernames through a series of security verification steps. Unfortunately, this method has significant shortcomings, as weak passwords that are easy to remember can be guessed, while strong passwords are difficult to remember, and users tend to write them down. Current implementations of single-factor authentication improve security by adding an additional step, an out-of-bound channel, usually through sending an authentication code via email or short message service (SMS).

A two-factor authentication (2FA) mechanism uses any two of the three approaches for identification and authentication, but mainly consists of SFA and 'something you have'. An example of this approach is the use of bank cards to access account information and withdraw cash in automated teller machine (ATM) systems. The user supplies the bank card and enters the PIN for identification and authentication, respectively. The online version of this approach uses token hardware, where a server generates a code and sends it to the hardware token. The user enters the matching code on the website to complete the authentication process. This approach increases the complexity of the system by adding token hardware management. Research has shown that this method has a negative impact on system usability, convenience, and ease of use from the users' perspective (Krol, Philippou, De Cristofaro & Sasse 2015). For example, a user effectively loses access to his/her online banking service until a lost token has been replaced.

Three-factor authentication (3FA) uses all three approaches, including biometric ('something you are') technology, such as a fingerprint scanner or voice recognition, to verify identity (Bhattacharyya, Ranjan, Alisherov & Choi 2009). There are a number of problems with biometric technology, including performance and accuracy with respect to balancing the cost of 'false rejection' and 'false acceptance' (Patel, Chellappa, Chandra & Barbello 2016) and spoofing attacks (Hadid, Evans, Marcel & Fierrez 2015). Biometric technology is still costly to implement, although the cost has recently been dropping to make it more feasible (Bonneau, Herley, Van Oorschot & Stajano 2012). Furthermore, an earlier study found biometric systems are perceived as intrusive by some sensitive users; for instance, some users are hesitant to touch a fingerprint scanner that has been touched by many other users (Matyas & Riha 2002). There are still logistical problems with biometric online authentication, especially on desktop computers. The advent of touchscreen smartphones is now making it possible to use some biometric mechanisms for online user authentication (Angulo & Wästlund 2012). Authorisation checks the levels the authenticated entity is allowed to access when granting access to information assets. Lastly, accountability ensures that all actions can be attributed to an authenticated identity (Whitman & Mattord 2017). Most systems use system logs to provide an audit trail. These need to be protected to prevent unauthorised access and modification in order to maintain their integrity.

Cryptography is the science of keeping 'secret codes' (Stamp 2011). It is the practice of using encryption to conceal text (Pfleeger & Pfleeger 2015). Encryption is the process of encoding plaintext, so that its meaning is not obvious (Pfleeger & Pfleeger 2015). Cryptography has its roots in communications security in the old paradigm (Gollmann 2011) and is commonly used to safely transfer information across communication systems without compromising integrity and authenticity (Peltier 2014). Cryptography through encryption is used to provide four basic InfoSec functions: confidentiality, integrity, authentication, and non-repudiation (Peltier 2014). As such, cryptography plays an integral part in the provision of effective access control mechanisms to any system, be it an offline or online environment.

Online applications such as online banking rely on access control mechanisms to grant access both to the system through authentication and to system information once access has been granted. Access control ensures the integrity of the system by providing different entities with specific rights to system information. For example, administrators have greater control over system activities than general system users. Given that online applications such as online banking are meant to provide remote access to bank accounts of clients, access control plays a crucial role. Hence, any security measures for such applications begin by making sure that the authentication process is effective and usable. Once access has been granted, the client has access only to areas of the system that pertain to that particular client's information.

Research is currently being done into improving authentication techniques and making sure that these techniques are usable in order to avoid misuse and compromise of the system. Previous studies include work on the usability of sensor technology authentication (Chuang, Nguyen, Wang & Johnson 2013), the evolution of password authentication (Bonneau, Herley, Van Oorschot & Stajano 2015), the usability of two-factor authentication (Krol et al. 2015), and the emergence of multi-factor authentication (Van Hamme et al. 2017). The usability of authentication mechanisms is beyond the scope of this research, although it does investigate system design issues that ensure that authentication mechanisms imposed by the system do not place an unnecessary burden on users, which, in turn, might compromise user behaviour when interacting with InfoSec applications. Biometric technology is increasingly being introduced in access control systems, from building access to online application authentication. Using the technology acceptance model (TAM), Morosan (2012) found that hotel guests approve of the use of biometrics.

Financial institutions are experimenting with different mechanisms to secure authentication of online banking and other online payment systems, especially due to the increase in malware and social engineering attacks. Currently, various mechanisms are used, from simple one-factor mechanisms such as a simple username and password combination to more complex three-factor techniques that include biometrics. As a result of the pervasiveness of smartphone devices that have built-in biometric technology such as iris, face, and fingerprint scanners, biometric solutions are no longer too expensive to implement. Some South African banks such as FNB allow fingerprint authentication for access to the online banking application on devices that support biometric authentication.

Although biometric costs have been decreasing (Pons & Polak 2008), there are still significant challenges to the technology's mainstream implementation such as usability issues on smartphones (Bhagavatula, Ur, Iacovino, Kywe, Cranor & Savvides 2015) and privacy in public places, as noted earlier. Research into improving the reliability of non-intrusive biometric techniques such as 3D hand gestures and face recognition is ongoing (Vasiete, Chen, Char, Patel, Davis & Chellappa 2014). In the context of online banking, Plateaux, Lacharme, Jøsang, and Rosenberger (2014) propose the use of a device that allows the bank to realise authentication of the biometric information presented using OTP verification.

2.7 INFORMATION SECURITY RISKS AND THREATS

InfoSec risks and threats arise from a number of sources due to malicious intent or negligence by all kinds of system users – end-users or administrators. Therefore, system administrators need to be vigilant and guard against all kinds of risks. The Oxford Dictionary (2018) defines risk as "[exposure to] *the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility*". The need for InfoSec arises from the existence of InfoSec risks, threats, and vulnerabilities as conceptualised by Talabis and Martin (2013) and illustrated in Figure 2-3. Risk is the possibility that some incident or attack can cause damage to one's system (Gollmann 2011).

Talabis and Martin (2013) define a threat as an event, either an action or an inaction that leads to a negative or undesirable situation. InfoSec threats are actions by adversaries that have the potential to cause loss of, or harm to, an asset. These actions can be either intentional or unintentional (Whitman & Mattord 2017; Peltier 2014). A vulnerability is a weakness in a system that might be exploited accidentally or intentionally to cause harm or loss (Gollmann 2011). For example, a server without password access represents a system vulnerability. The existence of a vulnerability in a system makes it possible for a security threat to be carried out successfully by exploiting that vulnerability.

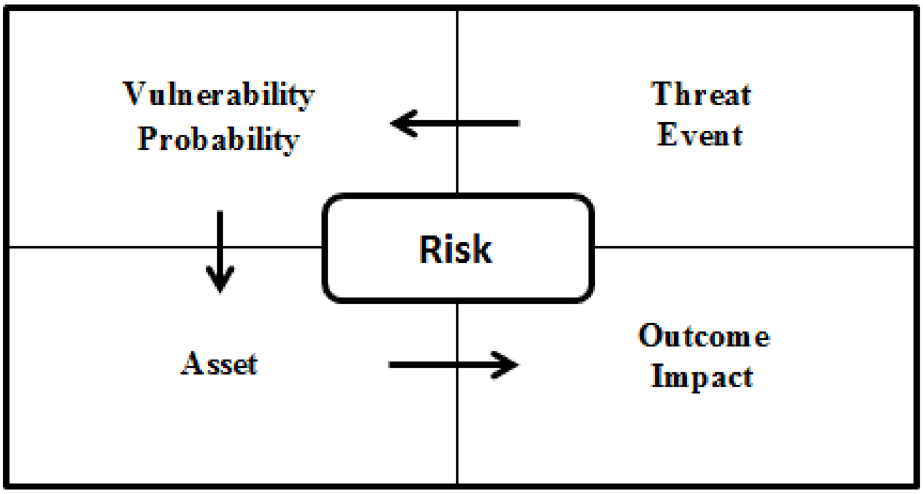


Figure 2-3: Risk and information security concepts (Talabis & Martin 2013)

Impact is the outcome such as loss or the potential for loss due to the threat leveraging the vulnerability (Talabis & Martin 2013). An example is unauthorised access to personal customer information. In essence, a threat is a possible danger that might exploit a vulnerability such as the existence of hackers. Figure 2-3 illustrates the relationships among three important concepts in InfoSec risk, namely, threats, vulnerabilities, and impact, as they apply to information assets.

Information assets are increasingly at risk from natural, unintentional, and intentional threats. Organisations and individuals must minimise risk to match their risk appetite, which is the quantity and nature of risk they are willing to accept (Whitman & Mattord 2017). With the increase in remote and online activities, there is an increase in risks and threats to, and vulnerabilities of, information assets, which compromises InfoSec and privacy for organisations and individuals alike. This calls for increased awareness for effective protection of information assets of organisations and individuals. The design of secure and usable online InfoSec applications reduces system vulnerabilities by addressing aspects that might open the systems to InfoSec risks. Usable IS applications also mitigate InfoSec risks that might arise from system misuse. The same vulnerabilities are often exploited by attackers to gain unauthorised access to information assets. The STInfoSec framework is envisaged to assist in the development of online applications that minimise InfoSec risks by taking socio-technical aspects into consideration.

2.8 INFORMATION SECURITY ATTACKS

The main goal of all security systems is to protect assets against possible harm – intentional or accidental. This harm can come from a number of possible sources, and the main categories are security threats and security attacks. The existence of security vulnerabilities and threats, as discussed earlier, increases the probability of a security attack occurring. There are various kinds of security attacks on ISs and information assets. These vary from software bugs and design flaws to outside attacks by hackers, who exploit such flaws and also target the gullible nature of human beings with attacks through social engineering.

In RFC 2828, Shirey (2000) defines an attack in the context of security as "*an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system*". According to Stallings (2011b), a security attack is any action that compromises the security of information owned by an organisation, and these attacks can be either passive or active. In a passive attack, the assailant only eavesdrops on the communication between the sender and the receiver to gain information about the conversation and to later use this for malicious purposes. Examples of passive attacks are wiretapping and port scanning. In an active attack, the assailant attempts to modify, redirect, block, or destroy the data, devices, or communication links (Stallings 2011a). Examples of active attacks are denial-of-service, masquerading, and spoofing attacks.

Security attacks can originate from two main sources: insider or outsider attacks. An insider attack refers to threats emanating from an entity with access rights to a system, and these privileges are misused, resulting in a violation of the security policy of the organisation (Theoharidou, Kokolakis, Karyda & Kiountouzis 2005). This attack can be performed by disgruntled employees, authorised vendors, or employees with just criminal intent for financial gains. An example of insider attacks is recent SIM-swap fraud incidents, where cellphone service provider employees collude with online banking cybercriminals to intercept OTP messages sent to cellphones for authentication of online banking transactions. An outsider attack is one originating from outside the perimeter of the organisation from an entity not authorised to access the system such as a hacker. Such attacks usually exploit system vulnerabilities in design or use brute-force attack techniques, such as password cracking.

What is certain, however, is that organisations have to guard against InfoSec threats from both outsiders and insiders when protecting organisational digital assets and that major threats come from insiders (Hu et al. 2012). With the advent of social engineering, outsider attackers gain access through the exploitation of insiders. Surveys from security technical reports and empirical research studies suggest that more damaging breaches are caused by the actions of internal employees than outside hackers (Crossler et al. 2013). It is worth noting that most insider threats are not considered intentional, but unintentional mistakes (Stanton & Stam 2006). Hence, it is vital to address the causes of such unintentional mistakes, and system design and usability go a long way to mitigate these mistakes and minimise system attack vectors, especially considering that the human element in InfoSec is emerging as a significant attack vector for exploitation (Rege 2016). InfoSec attacks are on the rise and are becoming more complex. Admittedly, there is no one solution to all InfoSec problems; however, a socio-technical approach to IS design can mitigate the human element attack vector by making applications both secure and usable.

2.9 ONLINE SECURITY

The internet currently experiences unprecedented daily traffic figures, driven by the huge social networking presence of providers such as Facebook, Twitter, Google, Tumblr, and Instagram, which constitutes millions of active daily users (Internet Live Stats 2018). The advent of smartphones has given a large number of users access to the internet, with huge transfers of data, of which some are sensitive and confidential in nature. Hence, the internet has become a honeypot for organised cybercriminal syndicates that prey on unsuspecting internet users, some of whom are novice computer users without basic InfoSec awareness knowledge (Choo 2008; Choo & Smith 2008). The ever-present nature of online computer users with different levels of security awareness makes social engineering attacks such as phishing more prevalent and more successful through social networking platforms.

Online security (also known as internet security) is the sub-field of computer or information security that is related to the internet and its related protocols, including network security (Walker 2014). It arises from the need to protect the internet as a transmission medium. Online security involves securing the internet and all its technologies such as the browser, since the internet is an open and public computer network with computers interconnected globally. For governments and organisations, as well as their clients, who conduct business online, online security is a major concern. Almost all organisations –

small or big, public or private – have some form of online presence. Military organisations of governments conduct sensitive and critical national security operations on the internet, and individuals perform confidential daily activities online. All of these activities need protection against the prying eyes of cybercriminals. Cheswick, Bellovin, and Rubin (2003) identify a number of classes of attacks such as the stealing of passwords, malware, authentication failures, information leakage, DDoS, botnets, and active attacks.

2.9.1 Cybercrime

Cybercrime or computer crime is crime committed in cyberspace, that is, against computers and computer networks using computer technology (Clough 2010). Specifically, Loader and Thomas (2013:3) define cybercrime as "*computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks*". Stallings (2011a) differentiates the term 'cybercrime' from 'computer crime', as he defines cybercrime as a crime that specifically occurs in cyberspace – thus, using computer networks – while computer crime may or may not involve computer networks. In the context of online InfoSec and this research, the term 'cybercrime' is not differentiated from 'computer crime', as a security breach through computer crime can facilitate a cybercrime attack.

Cybercrime is a global problem and a major threat to online security. There has not been an agreed definition of 'cyberattack', and the term has been defined based on a number of contexts such as the military, national security, and business. Generally, cyberattacks are deliberate actions against information assets in ISs or computer networks. These actions may destroy, disrupt, degrade, or deny access (Denning & Denning 2010).

Currently, cybercrime is organised, prompting governments and non-profit organisations to invest financially in initiatives to actively engage in countermeasures (Ben-Itzhak 2009). By its nature, cybercrime is a global problem, and international organisations and governments have joined forces to fight it. The United Nations (UN), the European Union (EU), and the Council of Europe, among others, have global initiatives to provide awareness and countermeasures for fighting cybercrime. They categorise cybercrime under economic crime due to its considerable impact on economic activities of citizens.

Unfortunately, the definition of cybercrime and what exactly constitutes it are not globally regulated, with some countries such as South Africa yet to pass laws that accurately define and prosecute cybercrime. Hence, cybercriminals take advantage of these gaps, especially in countries where cybercrime regulations are lagging (Glasser & Taneja 2015, Haase 2015). Cybercrime is a global business operated by international syndicates, costing the world economy billions of dollars, although there is no consensus on the exact figure. Current estimates from different sources differ significantly (Armin, Thompson, Ariu, Giacinto, Roli & Kijewski 2015, Hyman 2013).

The United States of America (USA) and United Kingdom (UK) have computer crime regulations that list the following crimes as computer crimes: theft of computer services, unauthorised access to protected computers, software piracy, alteration or theft of electronically stored information, extortion committed with the assistance of computers, obtaining unauthorised access to records from banks, credit card issuers, or customer reporting agencies, traffic in stolen passwords, and transmission of destructive viruses or commands (Casey 2011).

The cost of cybercrime in financial terms is increasing at an alarming rate based on available records. Forbes reports that cybercrime cost the global economy over US$ 450 billion in 2016 (Graham 2017), up from US$ 100 billion in 2013 (Morgan 2016). These figures include direct losses and post-attack disruption to normal business. The figure is projected to be US$ 2.1 trillion globally by 2019 (Graham 2017). In 2016, over two billion personal records were stolen globally, with over 100 million personal medical records stolen in the US alone (Morgan 2016). In South Africa, cybercrime cost the economy R35 billion in 2015, and 8.8 million South Africans were victims of cybercrime (IOL 2016). Cybercrime is expected to cost South African businesses up to R78 trillion by 2021 (Venktess 2017). SABRIC reported an overall increase in card fraud of 13% to R374.4 million in 2016 (SABRIC 2017). These figures highlight the financial impact cybercrime has on the global economy. Some of these security attacks are due to design flaws in, and misuse of, systems.

2.9.2 Malware

Organised cybercriminals use various types of malware to illegally obtain personal and financial information from organisations and individuals. Choo (2011b) identifies malware and phishing as the two biggest online threats to consumers and organisations. Sophisticated cybercriminals develop a multitude of malware and distribute this through spam phishing emails to facilitate cyberattacks on organisations and individuals. Malware is a broader term that includes security threats such as viruses, worms, Trojan horses, and backdoors, to mention just a few. Choo (2011a) categorises malware largely according to two groups: generic malware that targets the general population and customised information-stealing malware targeting specific institutions. Malware and phishing protection is not only a technical problem, but also involves the human factor, making awareness and education/training critical in any threat-mitigation approach. In 2014, 28 billion spam emails were circulating worldwide daily (Symantec 2015).

2.9.3 Social networking sites

Boyd and Ellison (2007:211) define social networking sites (SNSs) as:

> "[w]*eb-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system*".

Social networking services have grown rapidly, and currently, social networking websites dominate the top 10 most-visited websites (Alexa 2018). Facebook is the largest social network, with close to two billion active users (Internet Live Stats 2018).

Social networking sites are used to create social networks among people who share common interests; hence, maintaining total privacy once on social networks is difficult. For example, most settings of Facebook are opt-in by default, including those on privacy, requiring users to amend these settings to improve their online security and privacy (Comer, McKelvey & Curran 2012).

Social networking websites and services are used by a multitude of users from different generations and cultures. Organisations use SNS services to promote new products and services and maintain a social presence with their clients and customers (Zhuang, Hsu, Brewer & Xiao 2012). Individuals use SNSs to connect with friends and family and also to follow organisations and brands of interest. The services provided on SNSs include instant messaging, blogging, and picture and video uploading.

Social networking websites allow users to communicate and share information. These services provide cybercriminals with a means to reach out to victims and distribute malware for the sole purpose of stealing personal information. Security and privacy implications of participating in social networks are an ongoing research area. Saridakis, Benson, Ezingeard, and Tennakoon (2015) found that cybercrime could be alleviated by improving the awareness and skills of users regarding control of personal information disclosure and by increasing service security controls on social media websites. The privacy concerns of Facebook users have a direct impact on information sharing (Dhami, Agarwal, Chakraborty, Singh & Minj 2013), which makes users aware of security risks of posting personal information.

Attackers can solicit and gather personal information from SNS users' posts, and this information can be used for identity theft purposes. Shared links among trusted users on SNSs can also be used for social media phishing purposes in social engineering attacks. It is important to only invite people you know to join your social networks on SNSs, as publicly available information on the networks can be used to initiate identity theft and spear-phishing attacks (Chaudhry, Chaudhry & Rittenhouse 2016, Jagatic, Johnson, Jakobsson & Menczer 2007).

2.9.4 Social engineering

Social engineering is a non-technical security attack that makes users compromise computer systems by manipulating them into divulging confidential information (Krombholz, Hobel, Huber & Weippl 2015). Depending on how persuasive and convincing the social engineer is, the user can even be manipulated to carry out the malicious attack. Social engineering uses psychological vulnerabilities and triggers to influence the individual's emotional state and cognitive abilities to obtain information (Mouton, Malan, Kimppa & Venter 2015). This makes social engineering a difficult kind of threat to mitigate, as technical protection measures are usually ineffective against this kind of attack.

Social engineering attacks usually target online users in an attempt to make them disclose sensitive information about themselves or other parties. The information is then used maliciously to harm individuals and organisations. Users need to be taught how to identify potential attacks and how to reduce their chances of becoming a victim (Parsons et al. 2010). A common social engineering attack discussed later is phishing, which uses spoofed emails claiming to be from legitimate organisations, directing users to bogus websites with the intention of tricking recipients into revealing confidential login credentials.

Attackers who use social engineering cast their net very wide and hope to catch any susceptible victims who might lack the knowledge to identify the attack. With the current multiple devices always on online connectivity, there are numerous ways an attack can be initiated. Hence, users need to be aware and vigilant. What makes social engineering attacks difficult to prevent is that they rely on human behaviour, which changes often and cannot be predicted. Furthermore, for a social engineering attack on an organisation to be successful, all it takes is for one individual in the organisation to be gullible.

2.9.5 Identity theft

Simply put, identity theft is the illegal use of someone else's identification credentials to perpetrate economic fraud, such as obtaining credit (Saunders & Zucker 1999). Identity theft is regarded as the fastest-growing consumer fraud and happens both online and offline. With increased online activity by individuals, there is an increase in the amount of data people post online, making identity theft easy for criminals. Identity theft is, thus, emerging as a serious threat. For instance, in the USA, over 17 million adults have been victims of one or more incidents of identity theft (Harrell 2015). Hille, Walsh, and Cleveland (2015) explain the fear of online identity theft using a two-dimensional concept, involving fear of financial losses and fear of reputational damage. This suggests that consumers' participation in online shopping is negatively affected by the fear of online identity theft.

Offline identity theft can be mitigated through improved security checks by organisations; for instance, banks have begun to roll out security mechanisms that include biometric technology at branches to counter identity theft (Erasmus 2015). The online version of identity theft is proving more difficult to counter, as there are no satisfactory and main-stream biometric solutions yet that are foolproof. Edwards (2014) suggests authentication mechanisms that entirely require biometric attributes for successful protection against identity theft in cyberspace.

2.9.6 Phishing

Phishing is essentially a form of social engineering attack in which an attacker uses spoofed emails to deceptively obtain sensitive information or install malware on victims' computers by impersonating a trustworthy third party (Hong 2012). The Oxford Dictionary (2018) defines phishing as "[a] *type of internet fraud in which a person impersonates a reputable company in order to persuade others to reveal personal information, such as passwords and credit numbers, online*". The Anti-Phishing Working Group (APWG) is a global industry, law enforcement, and government coalition focused on unifying the global response to cybercrime through the development of data resources, data standards, and model response systems and protocols for the private and public sectors. The APWG (2017) landing web page defines phishing as "[a] *criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials*". Phishing that targets specific organisations or individuals is known as spear phishing, as it uses specific information about the target victim (Hong 2012).

Globally, phishing has emerged as a serious threat to online security. The main goal of phishing is to gain access to personal and confidential information that allows the perpetrator to steal the identity of the victim. Armed with this information, the perpetrator can use it for financial gains or criminal activities. In essence, phishing becomes a tool for accomplishing identity theft. Millions of victims are conned each year through phishing attacks that use emails and other messaging services to solicit login credentials and personal identification information.

Although the estimates for the total global cost of phishing vary, RSA, a top security firm, identified 37 000 monthly phishing attacks in 2012, with an estimated annual financial loss of more than US$ 1.5 billion (RSA 2014). The cost of phishing for the month of December 2014 was estimated to be US$ 453 million (RSA 2015). RSA suggests that phishing is the top online threat for both consumers and organisations conducting financial transactions online. According to APWG (2017), payment and financial services are the industries most targeted by phishing attacks. Cybercrime reporting is not compulsory in South Africa; therefore, cybercrime figures are estimates. The South African Banking Risk Information Centre (SABRIC) is a non-profit organisation formed by the four major banks to assist banking and cash-in-transit companies to combat bank-related organised crime. SABRIC reported an increase in credit card fraud totalling R374.4 million for

2016. This figure represents an increase of 13% compared to 2015. In total, South Africa loses R2.2 billion from internet fraud and phishing attacks each year (SABRIC 2017).

Phishing works for a number of reasons, as attested to by several research studies as highlighted below. The main reason is that people lack knowledge regarding the basics of how computers and related applications work (Alsharnouby et al. 2015). The following are some of the reasons why phishing works:

- People have a tendency to judge a website's validity by its 'look-and-feel', which attackers can easily reproduce (Dhamija, Tygar & Hearst 2006).
- Many users do not understand security indicators in web browsers, and they trust websites without checking security indicators, such as the SSL padlock on browsers (Alsharnouby et al. 2015).
- Some users are aware of phishing, but awareness does not reduce their susceptibility or improve their identification of phishing attacks (Downs, Holbrook & Cranor 2006).
- The seriousness of the consequences of phishing does not predict users' behaviour (Downs, Holbrook & Cranor 2007).
- Identifying phishing on the user interface is difficult; hence, the current method of relying on users to detect phishing attacks is unreliable (Alsharnouby et al. 2015).

More importantly, Hong (2012) suggests that phishing works because of the poor usability of many interfaces that provide insufficient cues to judge the legitimacy of email messages and websites. The author, furthermore, asserts that a deeper understanding of end-user motivations, beliefs, and mental models is critical for building effective countermeasures. The nature of social engineering attacks makes awareness the most appropriate method for mitigating these attacks. Well-designed user security education and training can be effective in the real world (Sheng, Holbrook, Kumaraguru, Cranor & Downs 2010).

People are increasingly active online through SNS services, sharing a multitude of personal information, sometimes with privacy settings that make this information accessible to other users. Such behaviour exposes users to cyberattacks through social engineering, identity theft, and phishing, as cybercriminals collect this information and use it to attack other valuable online services such as online banking. Therefore, online users need to be vigilant about personal information sharing, and awareness campaigns are critical, as some users are novices without basic computer literacy or InfoSec awareness knowledge. Hence, to mitigate these security risks, developers of such online applications need to take human behaviour into considerations and assist users wherever possible. Given the magnitude of protecting online users, it is evident that the responsibility cannot be shouldered by application developers alone, but must also involve all stakeholders, including individual users and government. The main purpose of phishing is essentially to deliver malware (Sawyer, Finomore, Funke, Mancuso, Miller, Warm & Hancook 2015). With spear phishing tactics, cybercriminals increase their chances of successful attacks. User awareness is essential in mitigating such attacks, as technology alone is insufficient.

2.9.7 Perceived risk

The notion of perceived security risk plays an important role in altering people's perceptions and decision-making. Biswas and Biswas (2004:31) define perceived risk in an online shopping context as "*the nature and amount of uncertainty perceived by a consumer in contemplating a particular purchase decision*". According to Forsythe and Shi (2003), the perceived online shopping risk for users is the expectation of loss in a given electronic transaction. Cheng, Lam, and Yeung (2006) found perceived web security to be a major determinant of clients' adoption of online banking. Previous studies showed that perceived security risk was an important predictor of online banking adoption.

In the context of online banking, Aldás-Manzano, Lassala-Navarre, Ruiz-Mafe, and Sanz-Blas (2009), as well as Littler and Melanthiou (2006), demonstrate that perceived risk is a significant factor in online banking use. The authors expand the risk factor to four levels: security, performance, social, and privacy risks. Security risk is the most significant, as consumers fear financial loss. Most banks have developed secure online banking technologies to secure online transactions. Lack of awareness regarding the security of online banking keeps potential online banking users away from using the service (Yousafzai, Pallister & Foxall 2003). Hence, banks need to create strategies to tackle specific risk elements.

Overall, perceived security risk plays a significant role in influencing participation in online activities such as online shopping and online banking, as there is always some risk of financial loss associated with these activities, compared to brick-and-mortar transactions. This calls for strategies not only to mitigate cyberattacks, but also to alter users' perceptions of InfoSec altogether and clarify how users can play a part in creating a secure environment.

The development of online applications has to consider online InfoSec threats faced by organisations and individuals and employ strategies that assist users in mitigating such attacks. The STInfoSec framework proposed in this research provides principles that satisfy usable security properties for online InfoSec applications. The researcher argues that the above-mentioned online InfoSec threats can be mitigated by designing applications based on validated principles that foster effective use of applications.

2.10 ONLINE BANKING

Since the late 1990s, the financial landscape has changed through the use of internet technologies (Gkoutzinis 2006). The emergence of electronic banking (ebanking) services such as virtual banking, home banking, and online banking, which provide various banking activities through electronic channels, has revolutionised the industry (Turban et al. 2015). At first, there was distance banking, where financial services were offered over the telephone system, with a bank official performing transactions based on the directives of the client. This has since evolved into the current online banking service provided over the internet.

The number of online banking users has been growing throughout the world, as the convenience of using online banking to perform banking transactions throughout the day has an edge over previous delivery channels. Nonetheless, there are outstanding online banking issues that still need to be addressed to achieve the full benefits of the service. As much as adoption is increasing, the rate of adoption is not the same across different economies. For example, the rate of uptake in developed economies is significantly higher than in developing economies. There are still security and privacy risks associated with conducting financial activities online that need to be addressed, as cited by several previous studies (Mujinga, Eloff & Kroeze 2016, Montazemi & Qahri-Saremi 2015, Sikdar, Kumar & Makkad 2015, Tarhini, Mgbemena, Trab & Masa'Deh 2015). There have been significant advances in mitigating security concerns, but these need to be communicated to customers to alleviate fears and encourage adoption.

Financial services comprise the full range of functions performed by financial institutions, including, but not limited to, acceptance of deposits, loan applications, payment services, funds transfers, asset management, opening new accounts, and paying bills. Almost all ecommerce transactions require some form of financial payment to complete the transaction. Hence, payments are an integral part of doing business, be it online or in the old-fashioned way. Traditional payment systems such as cash, cheques, money orders, and manual credit cards are not effective or appropriate for online ecommerce payments. Online banking and other electronic payment systems allow for electronic payments that fit perfectly in the ecommerce model. The wide range of services offered through online banking makes banking convenient and saves customers time. Gkoutzinis (2006) gives slightly different definitions of ‘ebanking’ and ‘online banking’. He views ebanking as covering a wider range of banking services, including ATMs and telephone banking.

Gkoutzinis (2006:7) defines ebanking as “*the provision of banking services and the initiation and performance of payments through the banking system by electronic means and other advanced technologies*”. Therefore, online banking is the provision of ebanking services over a computer network, such as the internet, through a computer or other access device with internet capabilities (Gkoutzinis 2006). Ebanking can be offered through a variety of communication methods and access devices, as depicted in Figure 2-4.

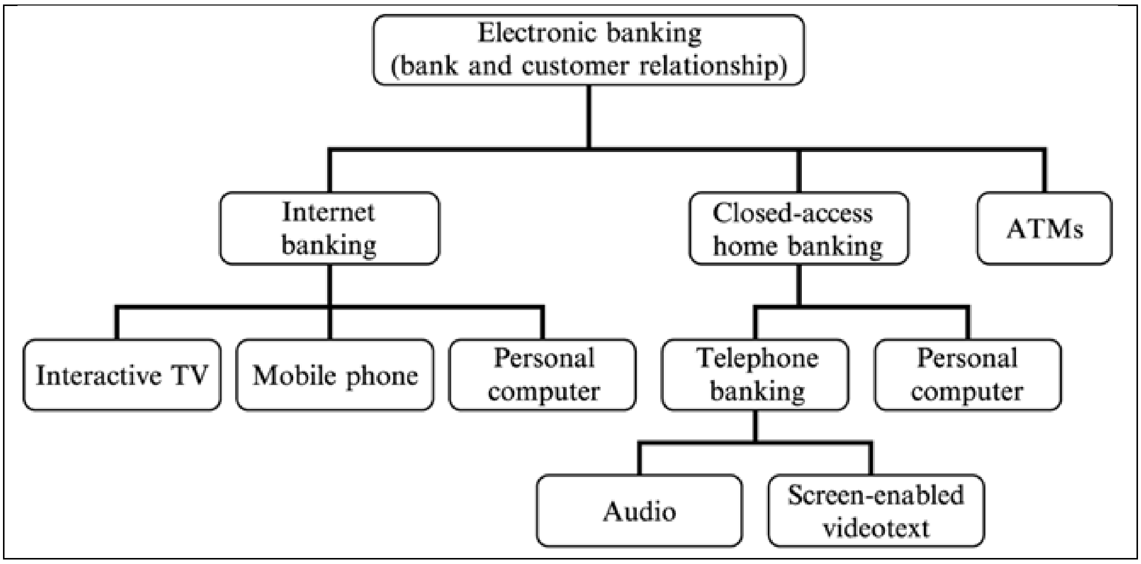


Figure 2-4: Communication methods and access devices (Gkoutzinis 2006)

Online banking, specifically the use of technological services in banking, has seen banking institutions reduce back-office and front-desk costs, resulting in increased customer satisfaction (Berger 2003). Shah and Siddiqui (2006) identify the following as some of the most critical for success factors in online banking: an understanding of customers, availability of resources, systems security, an established brand name, multiple integrated channels, good customer service, and systems integration. Customer adoption of online banking has been on the increase worldwide, driven by the perceived benefits of convenience (Vatanasombut, Igbaria, Stylianou & Rodgers 2008) and reduced costs (Hernando & Nieto 2007). Yet banks and online banking users have increasingly been targeted by cybercriminals, alerting banks to stepping up security systems. Users cite the perceived lack of security in online banking as an obstacle to adoption, even if their security fears are not based on actual experience. This can be attributed to the wide media coverage of some notable security and privacy breaches.

Among the factors affecting online banking adoption, Poon (2008) identified these 10 determinants in Malaysia: convenience, accessibility, speed, feature availability, bank management and image, content, security, privacy, design, and fees and charges. The study also revealed that security, privacy, and convenience were significant factors that facilitated users' acceptance of online banking.

2.10.1 Online banking in South Africa

The population of South Africa is approximately 55.91 million, with an adult population of around 37 million, based on 2016 estimates (Stats SA 2016). The country has an internet penetration rate of 49%, meaning that 27 million South Africans are internet users. Of the 36.8 million adults, 27.5 million (75%) have bank accounts (FinMark Trust 2016). Of these adults with bank accounts, 14 million have internet access, but only 2.3 million, which is less than 9%, use online banking services (Van Zyl 2015). This represents a worryingly low level of adoption of the service.

Compared to the rest of the world, South Africa has a very low adoption rate of online banking. In the US, 67% of the internet audience used digital banking in 2016 – a rise from 51% the previous year (Gonzalez-Garcia 2017). In comparison with 2014 figures, 49% of the total internet audience of European Union countries accessed online banking (Statista 2015), while the global average in 2012 was 28.7% of the internet audience (Statista 2012). Africa and the Middle East had 8.8% of internet users using online banking, with South Africa recording only 8.5% (Statista 2012). The online banking penetration rate for South Africa and the African region is far lower than the global average.

A recent survey indicated that 43% of internet users in South Africa considered branch banking to be safer than online banking, with 64% feeling vulnerable when doing financial transactions online (FinMark Trust 2016). Moreover, just less than half (49%) reported that they believed making payments offline was more reliable than online, and 43% agreed that offline banking was safer than online banking.

Regardless, internet users worldwide conduct online banking transactions from a variety of unsecure devices, without taking basic security measures such as setting up a device password to protect their online transactions (Kaspersky Lab & B2B International 2016). This puts both the users' finances and the bank's reputation at risk. The desktop is still the dominant device for online banking access, with 57% of users using it worldwide. The trend is similar for other online services such as online shopping, social media, and email, where the desktop continues to be the most-used device to access these services.

A Kaspersky Lab and B2B International (2016) survey found that a total of 75% of respondents believed that banks, payment systems, and online stores had to provide them with special solutions for secure transactions on their endpoints. Nonetheless, the survey also reported that users still practised unsafe behaviour, even if they were aware of, and worried about, online security threats. Furthermore, while fewer than 80% of computers were password protected, only just over half of smartphones and Android tablets had passwords. Given the obvious risks of free public Wi-Fi networks, only 38% of respondents took precautions when using such networks (Kaspersky Lab & B2B International 2016).

2.10.2 Threats to online banking security

The most-used tactic to get into online banking users' accounts is the use of phishing as a form of social engineering attack (Yee 2004a). Users essentially believe they are directed to the legitimate website of their trusted bank and proceed to log in, thereby providing their login credentials to the attacker. Phishing basically bypasses the organisation's security infrastructure such as firewalls and authentication mechanisms, as the attack is directed at authenticated users to obtain sensitive information.

Similarly, the attack can target the user with an email that installs a Trojan to collect login details when entered into a legitimate bank website. This tactic uses a banking Trojan to intercept the username and password. Attackers can also pose as the legitimate account owner, using identity theft. This can be done by getting information about the account through setting up a phishing page where users unwittingly hand over their usernames and passwords. Computers and mobile devices are both vulnerable to these attacks.

The bank's terms and conditions for the provision of online banking often outline the contract between the bank and the customer to govern online banking service usage. From the point of view of the banks, security is vital to maintain their brand name and limit liability as a result of possible security breaches, while being compliant with rules and regulations that govern the industry. Sadly, this means that usability and UX come second and are second best. Given the immaturity of some of the legal frameworks that govern cyberspace and online transactions, loopholes are exploited to circumvent liability for online fraud. Hence, it has emerged as a huge competitive advantage to actually be able to provide security and acceptable usability and UX.

The significant role played by InfoSec problems as a barrier to the adoption of services such as online banking calls for ideas on how to alleviate fears of users concerning InfoSec risks. Attacks on online banking through the tactics mentioned earlier such as social engineering, identity theft, and successful delivery of malware through phishing pose huge risks to users and financial organisations alike. The researcher investigated the role played by InfoSec and usability in adoption and continued use of online banking with regard to user interaction with InfoSec mechanisms. The ever-increasing online InfoSec threats and the vulnerability of novice users call for design and development approaches of online applications that take into account the intricacies of the online security environment, while – at the same time – being usable by the ordinary user. The researcher endeavoured to develop a socio-technical design framework that sought to address all aspects of online application development, taking user behaviour into consideration. This research looked at these different aspects through a socio-technical lens and proposed a framework to assist in the development of secure and usable online applications. The STInfoSec framework suggests usable security design principles, accompanied by checklist items for each principle. The principles satisfy usable security properties in designing online InfoSec applications thereby assisting user to mitigate online banking InfoSec threats.

2.11 CHAPTER CONCLUSION

The technical need to secure personal information of users, especially in sensitive online applications, requires a multifaceted approach to different aspects. In the current environment, online security threats are becoming more complicated and are created in large numbers. This, coupled with the diverse computer and InfoSec awareness skills of the average online user, makes the design of sensitive online applications critical in mitigating security breaches. This chapter addressed the technical challenges of designing a socio-technical system. There are several layers of security to be addressed, and a breach of any one of these layers renders all protections invalid. Hence, InfoSec relies on the effectiveness of all five other layers, as pointed out by Whitman and Mattord (2017). In the InfoSec layer, there is a collection of principles anchored by the CIA triad, each of which needs individual attention for a holistic solution.

The cornerstone of any online application, especially applications that disseminate sensitive information, is access control through the principle of authentication. The usability of authentication mechanisms is a fully fledged stand-alone research area that has existed for decades. At present, innovative technology such as biometrics is being considered for online authentication. Current major threats to personal information stored online are social engineering attacks that literally bypass any state-of-the-art protections and deceive users into revealing confidential credentials that allow access to systems.

This research used online banking as the case study online application mainly because, in South Africa, the adoption rate of the service is less than the global average. The service also meets the characteristics of a sensitive online application, since it involves transmission of personal and financial information through a public medium: the internet. The aim of this chapter was to identify and characterise the nature of online applications and the prevalent threats to these applications, highlighting attack vectors such as social engineering and identity theft. Chapter 3 covers the literature review, which was used to gather information for the development of the preliminary framework.

-- oOo --

CHAPTER 3 FRAMEWORK DEVELOPMENT

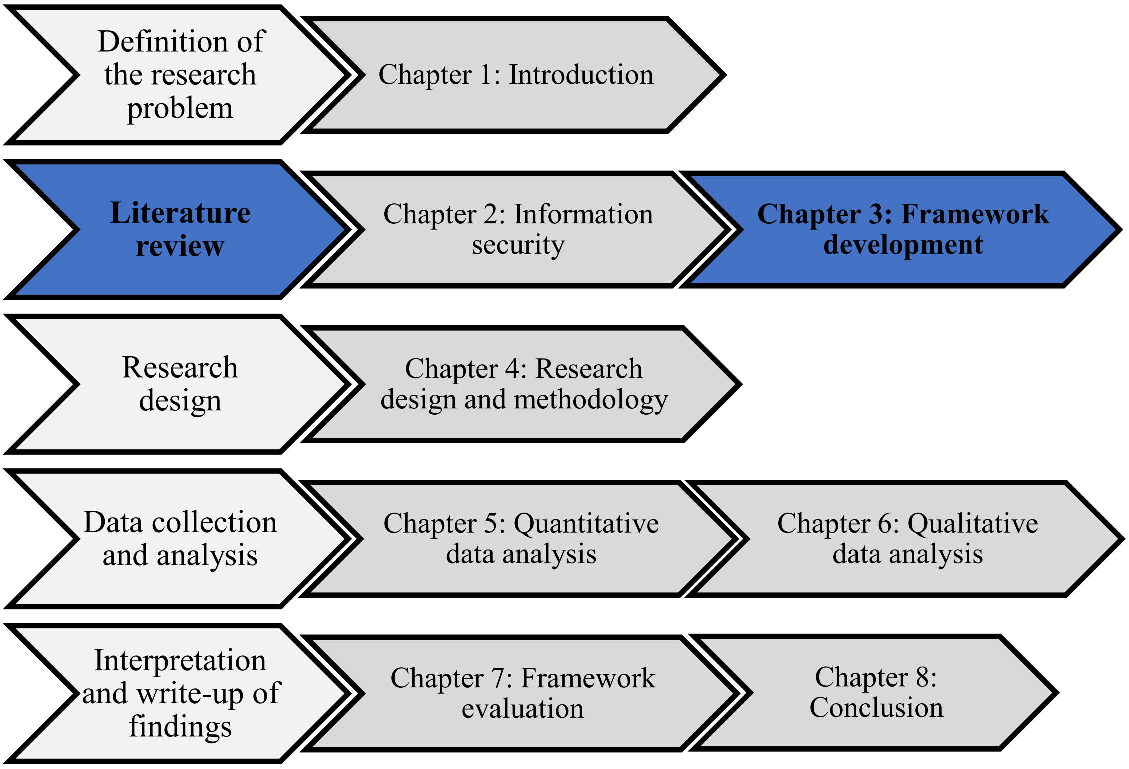

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 3-1: The research roadmap

3.1 INTRODUCTION

The relationship between humans and computers has existed since the introduction of computers. Although users were just glad to have computing power to perform basic tasks at the beginning, as time passed and computers evolved, it became apparent that computer functionality alone was not enough. This led to the introduction of the field of human-computer interaction (HCI) and more emphasis on system usability. This research work falls into the human-computer interaction security (HCISec) or usable security category, where HCI meets InfoSec. Usable security involves the application of usability design principles in the design and development of InfoSec mechanisms in an IS application.

The main goal of usable security is to enable users to use InfoSec mechanisms in order to mitigate InfoSec risks through effective use of applications. Ultimately, having InfoSec systems that users can use helps to create a viable security culture in an organisation and society at large. The previous chapter discussed the technical aspects of securing online applications. This chapter provides a critical discussion of the social aspects of the InfoSec problem in the context of online InfoSec applications, before the presentation of the preliminary STInfoSec framework. The two chapters combined complete the literature review of this socio-technical approach to designing online InfoSec applications.

The researcher argued that, for a holistic solution to InfoSec problems, both technical and social aspects needed equal attention in IS design. The proposed STInfoSec framework for the design of secure and usable online InfoSec applications, therefore, consisted of validated design principles. This chapter provides a critical discussion of design principles in the literature that guided the selection of those principles selected for investigation in the study.

3.2 HUMAN-COMPUTER INTERACTION

HCI is an interdisciplinary field associated with a number of other fields of study, all with the goal of designing computer technology that is easy and pleasant to use. Related fields of study include computer science, cognitive science, and psychology, to mention just a few. There are various definitions of HCI, with the notable ones included here. According to ACM SIGCHI (1992:5), HCI is "[a] *discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them*". HCI relates to how humans interact with computer technology in their everyday work and other activities. Broadly speaking, computer technology involves any devices with computing capabilities. Apart from computers themselves, other devices include mobile phones and appliances.

The concept of considering human factors in the design of equipment started during World War II, and it developed into HCI in the late 1960s, just after the introduction of mainframe computers (Grudin 2012). HCI has evolved rapidly over time. Figure 3-2 illustrates the timeline of the evolution of human factors, ergonomics, ISs, and HCI during the century between 1905 and 2005.

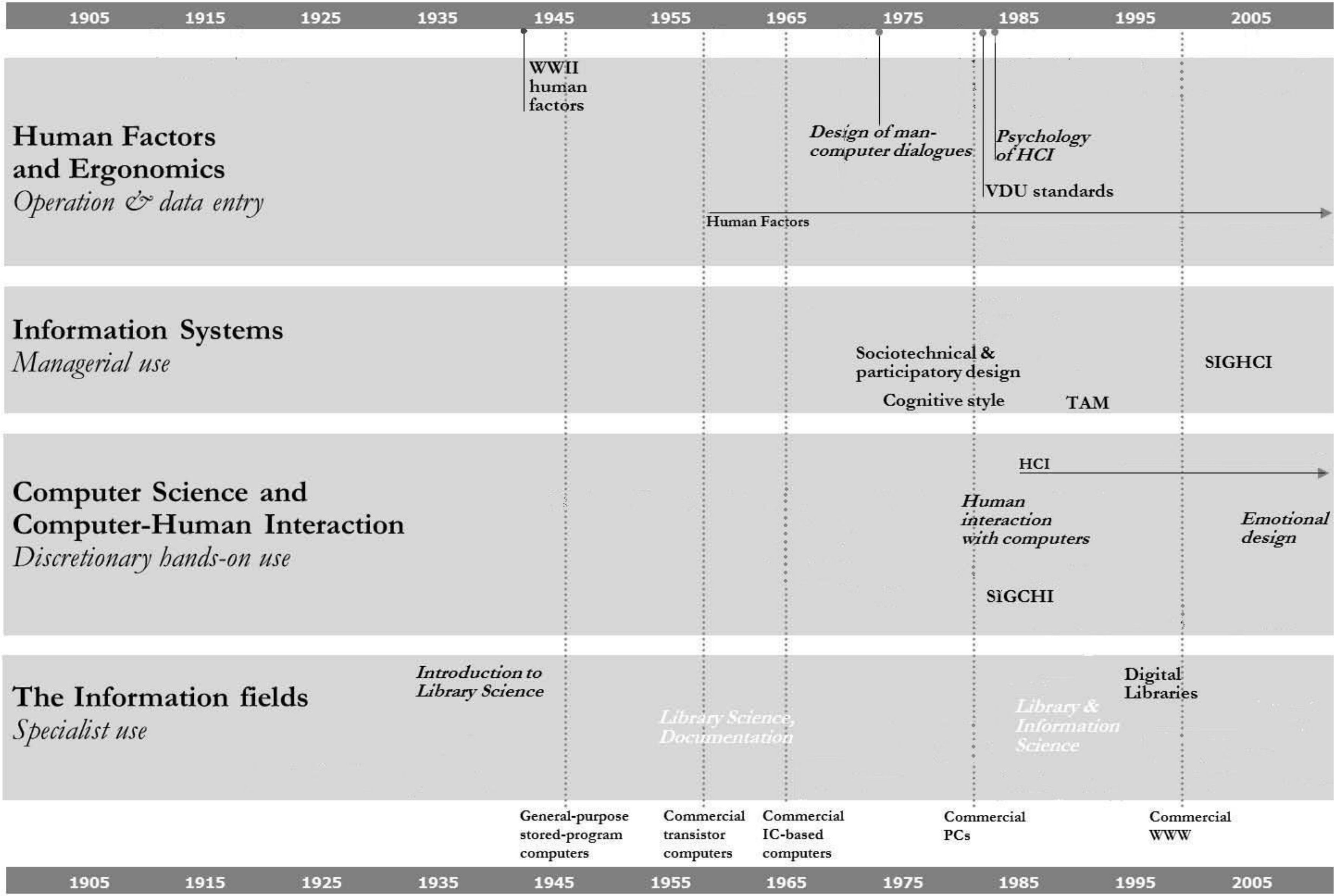

1905
1915
1925
1935
1945
1955
1965
1975
1985
1995
2005
Human Factors and Ergonomics
Operation & data entry
WWII human factors
Design of man-computer dialogues
Psychology of HCI
VDU standards
Human Factors
Information Systems
Managerial use
Sociotechnical & participatory design
Cognitive style
TAM
SIGHCI
Computer Science and Computer-Human Interaction
Discretionary hands-on use
HCI
Human interaction with computers
Emotional design
SIGCHI
The Information fields
Specialist use
Introduction to Library Science
Library Science, Documentation
Library & Information Science
Digital Libraries
General-purpose stored-program computers
Commercial transistor computers
Commercial IC-based computers
Commercial PCs
Commercial WWW

Figure 3-2: HCI events and topics (Grudin 2012)

Liu, Goncalves, Ferreira, Xiao, Hosio, and Kostakos (2014) presented a comparison of two decades of articles and keywords at ACM's CHI Conference on Human Computer Interaction, which has been running since 1982 and is one of the leading conferences in the field of HCI. Their comparison was between the periods 1994 to 2003 and 2004 to 2013 to identify the landscape of the field. Usability appeared significantly in both periods, while security was only prevalent in the second period, especially due to the influx of mobile devices (Liu et al. 2014).

The following sections detail the evolution of HCI and other related terms, thus providing the context of the current trend of usable security design – the subject of this research.

3.2.1 Human factors and ergonomics

Human factors and ergonomics are important wherever people work with systems, be these social or technical in nature. The range of such socio-technical systems includes system elements such as tools, software, tasks, and environments. Human factors are concerned with how people interact with these systems in their workplace. The International Ergonomics Association (IEA) gives a combined definition of ergonomics (or human factors) on its homepage as (IEA 2018):

> "*the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data, and methods to design in order to optimise human well-being and overall system performance*".

It is important to note that this definition does not single out any particular type of system; the field applies to any system, be it machinery or a software application. In the context of information technology, designers are more concerned with human factor aspects than strict ergonomics issues, since human factors specifically address concerns about how technology and computers, in particular, are integrated in the workplace to achieve optimum productivity for the user.

Human factors in InfoSec are factors that can improve the use of InfoSec systems or the features of these systems or that can deter users from using them. The focus is on a design that fosters optimum use of system features, particularly security features. If designers fail to address human factors in security, users will misuse the systems, as they will bypass security mechanisms, thereby creating an unsecure environment.

3.2.2 Mental models

The term ‘mental model’ was first coined in cognitive psychology and is now extensively applied in HCI to explain human behaviour. Users’ behaviour in relation to information systems can be explained through the content of their knowledge, including their theories and beliefs (Payne 2012). Fulfilling expectations depends on keeping behaviour and expectations in agreement, where user expectations are mainly influenced by users’ mental model of the system. Yee (2005; 2004a) asserts that security policy and the mental model are dynamic, since they change in response to user actions. Getting users to use InfoSec systems effectively is one of the key challenges (Dourish, Grinter, De la Flor & Joseph 2004). Hence, designers of information systems need to understand the mental model users have of the system’s capabilities and limitations to avoid a mismatch. This is even more important in InfoSec systems, as it might create an unsecure environment.

Understanding unique mental models users have of InfoSec and privacy issues online assists in understanding the problem and providing effective solutions. Prettyman, Furman, Theofanos, and Stanton (2015) found that online users had multiple and often contradictory mental models of their understanding of, and experience with, InfoSec and privacy. Therefore, a socio-technical approach ensures that proposed solutions provide an array of social aspects such as usability and user experience (UX), thereby addressing some of the multiple mental models held by users.

3.2.3 Memory load

Humans are not machines. The human mind can only hold and recall a certain amount of information, which varies significantly from one person to another. According to Proctor and Vu (2012:30), memory *“refers to explicit recollection of information in the absence of the original stimulus and persisting effects of that information on information processing that may be implicit*”. Short-term memory (STM), also known as working memory, refers to “*representations that are presently being used or have recently been used and that last for a short period*” (Proctor & Vu 2012). Therefore, users of information systems often utilise STM to remember things such as usernames, passwords, PINs, and essentially how to use these systems. It is imperative that system designers do not overload the STM. This is even more important in InfoSec systems to avoid unsecure behaviour such as writing down passwords. Memory load was taken into consideration in the proposed STInfoSec framework by making sure that the design enhanced learnability and provided help and documentation to users. This ensures the application is easy to use for repeat users and they will not have to learn the user interface all over again.

3.3 USABILITY

Usability is invisible, and it is the reason why users love certain products or services they use daily. As Barnum (2011:1) puts it, "[w]*hen usability is inherent in the products we use, it's invisible. We don't think about it. But we know it's there*". The absence of usability in a product or service brings about frustration; in extreme cases, users decide not to bother using the product or service. Preece et al. (2015) note that most gadgets are engineered to work effectively, while neglecting the usability aspects from the users' perspective. The same can be said of most software applications, even more so InfoSec systems. The introduction of usability early in the design process has become the norm to mitigate usability problems – hence, the suggestion by Mitnick and Simon (2002) that attackers are exploiting the human factors neglected by designers to gain access to computer systems.

One definition of usability that has become standard is the usability process-oriented approach from the ISO (ISO 9241-11 1998:6), namely, "*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use*". The definition highlights three key aspects: specific users, specified goals, and a specified context of use. The ISO also highlights the importance of the context of use in its definition of product-oriented usability. ISO/IEC 9126-1 (2001) defines usability with emphasis on the ability of users to understand, learn, and use a software product under specified conditions, while the Institute of Electrical and Electronics Engineers (IEEE) standard defines usability as the ease with which users can learn to operate the system (IEEE Std. 610.12 1990). In the context of product-oriented usability, product usability hinges on the user, the task, and the environment in which the product is being used.

Subsequent definitions of usability emphasise different usability attributes, as new insights have given rise to new attributes, since both researchers and practitioners have started to appreciate that usability has many facets. Nielsen (2010) states that usability is not one-dimensional and specifies five quality attributes of usability, namely, learnability, efficiency, memorability, errors, and satisfaction. Other authors such as Rubin and Chisnell (2008) characterise the usability of a product or service in terms of the following attributes: useful, efficient, effective, satisfying, learnable, and accessible. The main usability attributes as applied in usability studies are discussed in the following section.

In this research, the researcher incorporated both the process-oriented and product-oriented usability approaches to investigate the usability of online banking user interfaces, enabling users to achieve effectiveness, efficiency, and satisfaction from the service. Conversely, the researcher looked at the usability of the system as a product; that is, the interface needed to be learned, understood, and used and had to be satisfactory to the user. Rubin and Chisnell (2008:1) argue that what makes a system 'usable' is the *absence of frustration* while interacting with it. The authors go on to state that, when a product or service is truly usable, "*the user can do what he or she wants to do the way he or she expects to be able to do it, without hindrance, hesitation, or questions*" (Rubin & Chisnell 2008:3). This highlights the significance of understanding the user's mental model of the system in order to match system capabilities with user expectations. Nielsen (2010) explains usability as part of the larger issue of system acceptability, as depicted in Figure 3-3.

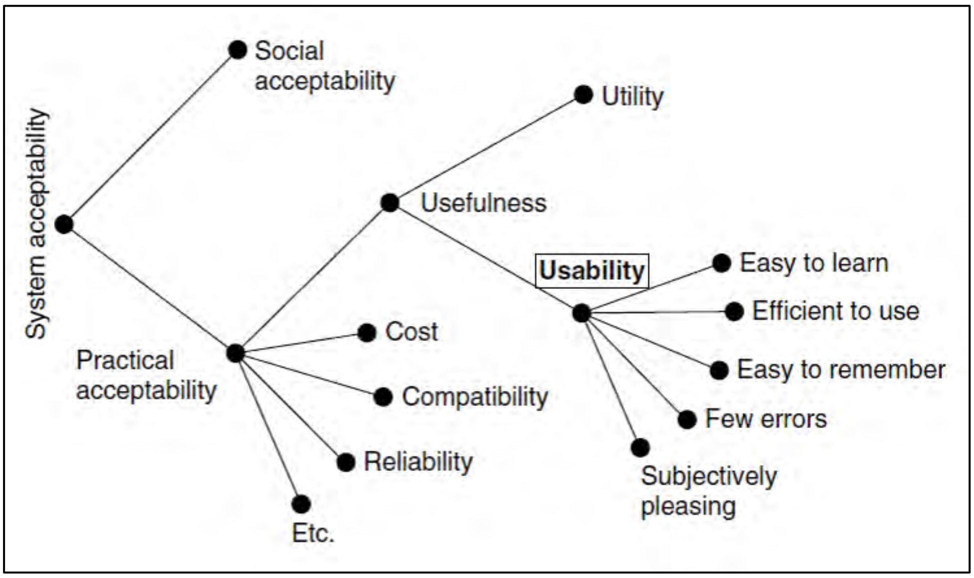


Figure 3-3: System acceptability attributes (Nielsen 2010)

Social acceptability and practical acceptability form part of system acceptability. Practical acceptability, furthermore, considers aspects such as reliability, compatibility, cost, and usefulness, to mention but a few. Usefulness is explained in terms of utility and usability, where utility assesses whether the system provides the intended functionality and usability considers how well users can use the system functionality (Nielsen 2010).

Online applications need to ensure that users get an experience that makes them come back by satisfying both their functional and sensory needs. These online applications offer the services through some form of interface – be it web or device (such as smartphone) applications. A number of usability goals were found in the literature. After an in-depth literature review, the researcher identified the most significant of these in the context of the current case study: online banking.

3.3.1 Error tolerance and prevention

The system should ensure that users make as few errors as possible, where an error is any action that does not achieve the wanted goal. The error rate is the number of errors users make during the use of a system while performing a specific task (Nielsen 2010). The system error rate should be low to prevent users from making many errors and to allow them to recover without catastrophic consequences (Nielsen 2010). This goal can be thought of as related to the safety goals that ensure that no serious harm can result from users making serious mistakes when using a product or service. In the context of online banking, this entails, for instance, avoiding errors such as paying the wrong beneficiary, which might cause serious inconvenience to users.

3.3.2 Satisfaction

Satisfaction refers to the users' perceptions, feelings, and opinions of the system, meaning that the users should be subjectively satisfied when using it (Nielsen 2010). This information is generally captured by means of both oral and written questioning (Rubin & Chisnell 2008). A system that meets users' needs and provides satisfaction allows users to perform well.

3.3.3 Learnability

Learnability is regarded as the most essential usability goal, since systems need to be easy to learn (Preece et al. 2015). The system should allow users to rapidly learn the design and quickly start to get some work done (Nielsen 2010). Rubin and Chisnell (2008) consider learnability as being linked to effectiveness, since users should be able to use the system after some period of training to some defined level of competence. Users prefer learning how to use a system by actually using it, especially online applications, as users are too impatient to read tutorial manuals.

3.3.4 Memorability

Memorability refers to the ability of a returning user to use a system without having to be trained for it all over again (Preece et al. 2015). A system with good learnability helps users to remember how to use it quickly. Apparently, interface memorability is one of the rarely evaluated usability attributes compared to other attributes (Nielsen 2010).

3.3.5 Usefulness

Usefulness is the ability of a system to achieve a specific desired goal(s) (Nielsen 2010). As mentioned earlier, Nielsen (2010) considers usability as a function of usefulness; thus, usefulness is not an attribute of usability (refer to Figure 3-3), since a system has to be useful first before looking at how usable it is to the user.

3.3.6 Safety

Safety protects the user against conditions and situations that may be undesirable and dangerous (Preece et al. 2015; Petrie & Bevan 2009). Safety as a usability goal was initially intended to protect people operating machinery in workplaces (ISO 9241-210 2010). In the context of software products, safety strives for reduced risk of harm to system users or other resources, including hardware or data. The ISO/IEC 9126-4 (2004) standard defines two aspects of software product safety. *Operational safety* enables a software product to meet user requirements during normal operation without harm to other resources and the environment, with attributes such as consistency, completeness, accuracy, insurance, and security. *Contingency safety* ensures that the product is capable of operating outside its normal operation, while still preventing risks, with attributes such as fault tolerance and resource safety. In general, safety ensures that no severe harm can result from users making serious mistakes when using a product or service.

3.3.7 Utility

Utility ensures that the product provides the right kind of functionality that allows users to complete their tasks (Preece et al. 2015). In other words, utility ensures that a product can deliver the intended results if used properly without obvious mistakes. For example, a calculator should give the correct sum of numbers if the numbers are entered correctly. As depicted in Figure 3-3, Nielsen (2010) places utility outside usability goals, arguing that usability is not an issue in products or services that have no functionality.

The usability goals presented here do not represent an exhaustive list, as there are numerous others for specific systems. The above list consists of the usability goals within the scope of this research. The order of importance of usability goals depends on system requirements and what designers perceive as necessary to achieve system goals. In the context of online InfoSec and the case study (online banking) of this research, in particular, the above list was deemed important in addressing usability problems. Although not all of the above principles were included in the final framework. There are also other goals that were deemed either implicit or outside the research scope, including effectiveness, efficiency, accessibility, universality, and flexibility, to mention but a few.

3.4 USER EXPERIENCE

Usability is a narrower concept that mainly focuses on the ability of the user to successfully complete some specific system task. In other words, usability is mainly concerned with the functionality of the system that allows the completion of a task (Albert & Tullis 2013). Since the permeation of technology in our daily lives, our main concern is not only the successful completion of tasks, but also enjoyment of the whole experience of system interaction, referred to as user experience (UX). UX takes a broader view than, and goes beyond, usability, in that it includes the user's entire interaction, including thoughts, feelings, and perceptions that result from interaction with the system (Albert & Tullis 2013). UX essentially includes aspects such as HCI, human factors, ergonomics, usability, and accessibility, which is more than just system usability (Hassenzahl, Platz, Burmester & Lehner 2000).

Therefore, the term 'user experience' has emerged to address aspects of users' interactions with systems that go beyond effectiveness, efficiency, and satisfaction (Petrie & Bevan 2009). In essence, usability is included in the broader realm of UX, as current systems seek to amuse and entertain users (Albert & Tullis 2013). Yet usability uses objective metrics for measurement, while UX is more about users' hedonic reactions, which are generally subjective, to the system (Petrie & Bevan 2009).

Law, Roto, Hassenzahl, Vermeeren, and Kort (2009) argue for the separation of UX from other experiences, such as the broader product experience and service experience, recommending that the term should exclusively refer to products, systems, services, and objects with which a user interacts through a user interface. Bevan (2008) advocates that usability can be extended to encompass UX by interpreting 'satisfaction in use', a subcharacteristic of usability, as proposed in ISO/IEC 25010 (2011), as a UX attribute. The four sub-characteristics are *likability*, deals with the satisfaction from the perceived achievement of pragmatic goals. *Pleasure* is the extent to which the user gains satisfaction from the perceived achievement of hedonic goals of stimulation, identification, evocation, and associated emotional responses. *Comfort* relates to satisfaction of physical comfort. Lastly, *trust* deals with satisfaction that the product will behave as intended. User satisfaction is usually measured using a psychometrically designed questionnaire for more reliable results (Hornbæk 2006).

Apart from usability goals, researchers and practitioners are now looking at improving interaction design systems to cater for additional goals such as UX. Compared to the more objective usability goals, UX goals are mostly subjective, since they are based on how users experience the product from their perspective (Preece et al. 2015). Preece et al. (2015) provide UX goals that include a wide range of emotions and felt experiences, grouped according to two categories: desirable and undesirable aspects. Table 3-1 lists some of these emotions.

Table 3-1: Aspects of user experience

Desirable aspects	Undesirable aspects
Enjoyable	Childish
Fun	Gimmicky
Satisfying	Frustrating
Entertaining	Annoying
Surprising	Boring
Challenging	Unpleasant
Rewarding	Patronising
Exciting	Cutesy
Pleasurable	Making one feel guilty
	Making one feel stupid

(Preece et al. 2015)

The list of UX goals in Table 3-1 is not exhaustive, as there are many more qualifying UX goals, given the highly subjective nature of UX. Hence, system designers do not need to cater for each and every UX goal users might come up with. Although that might be preferable, it is difficult and even impossible to achieve. In contrast, system designers should strive to eliminate all undesirable aspects from system design. Therefore, just as in the case of usability, the decision regarding which goals to include in the design of a system depends on the type of system and the aspects that are important to system designers. For example, the goals relevant to a system such as an online multiplayer game are different from those important in an ehealth application for patients and doctors. There are some goals that are important for any system such as being satisfying and enjoyable, which all systems should strive to achieve.

3.5 WEBSITE USABILITY

Website usability and its design principles are important in the context of this research, as online banking service is primarily provided through some form of web interface, be it computers or portable devices. The desktop is the leading device used to access the internet and online IS applications (Kaspersky Lab & B2B International 2014). This means that web usability (or, specifically, website usability) is still an important aspect of designing successful ecommerce portals. This is not only restricted to ecommerce, but includes any other portal that provides products, services, or information to users; examples include library catalogues and government portals for citizens. To quote Nielsen (2000:10), one of the main web usability authors, "[u]*sability rules the Web. Simply stated, if the customer can't find a product, then he or she will not buy it*". There is extensive research into what constitutes web usability, and this discussion is dominated by design principles that cater for user needs. Website usability strives to make a website easy to use, while UX aims to make the user happy before, during, and after using that website. Essentially, website usability, on the one hand, is concerned with users navigating the website with ease and being able to perform specific tasks. UX, on the other hand, focuses on the way users *perceive* their interaction while performing tasks on the website.

Usability principles are similar to design principles, the exception being that they are more prescriptive (Preece et al. 2015). Additionally, whereas design principles are mainly used for informing a design, usability principles also provide the framework for heuristic evaluation of system usability (Preece et al. 2015). Nielsen's 10 widely applied usability principles, which also overlap with design principles, include visibility of system status, the match between the system and the real world, user control and freedom, consistency and standards, helping users recognise, diagnose, and recover from errors, error prevention, recognition rather than recall, flexibility and efficiency of use, aesthetic and minimalist design, and help and documentation (Nielsen 1995).

The usability principles outlined in this section are generic and can be adapted to any kind of product or service, including user interfaces. Nonetheless, there are a number of studies that suggest usability principles specifically for website usability. Shneiderman, Plaisant, Cohen, Jacobs, Elmqvist, and Diakopoulos (2016) propose the following eight 'golden rules' widely adopted for interface design:

1. *Strive for consistency* for aspects such as layout, terminology, and command use.
2. *Enable frequent users to use short cuts* by allowing the use of abbreviations, special key sequences, and macros.
3. *Offer informative feedback* for every user action.
4. *Design dialogs to yield closure* to inform the user when a task has been completed.
5. *Offer error prevention and simple error handling* to prevent users from making mistakes in the first place, and provide clear error recovery instructions.
6. *Permit easy reversal of actions* to encourage exploration and relieve anxiety, as users can always return to the previous state.
7. *Support internal locus of control* that puts the user in control of the system.
8. *Reduce short-term memory load* by providing displays that are simple and multiple-page displays.

The design principles discussed so far are more or less meant to address usability and UX problems in interactive systems through the use of user-centred design approaches. The following sections discuss the notion of *usable security*, which is the cornerstone of this research. Website usability is critical in online applications as they are usually provided through some form of user interface on a variety of devices. As such, design of the user interface using a socio-technical approach that incorporates usable security properties is critical. The STInfoSec framework proposed in this research provides the usable security principles and checklist items to assist system designers in usable interface design.

3.6 USER-CENTRED INTERACTION DESIGN

Interactive computer systems are characterised by a significant amount of interaction between users and the computer. Interactive products include systems, technologies, environments, tools, applications, services, and devices with interactive characteristics (Preece et al. 2015). In 1975, Saltzer and Schroeder (1975) introduced the notion of design principles to improve security and protection of computer systems. They suggested that proper design mechanisms could improve access rights to information stored in computer systems and avoid unauthorised access. More recently, researchers and practitioners have given more attention to design principles in the development of products and services with which users interact directly. Design is now a main topic in creating user-friendly information systems that are usable and secure. A number of studies have proposed general design principles and best practices for usable information systems and specific usable security design principles for InfoSec systems.

Researchers and practitioners in the field of HCI and related disciplines have developed considerable empirical evidence material that designers can apply in user interface designs. Shneiderman et al. (2016) group the material into the following three categories: *guidelines* are specific and practical, prescribe good practices, and caution against dangers; *principles* are middle level and less prescriptive and analyse and compare design alternatives; and *theories and models* are high level and describe objects and actions with consistent terminology that allows comprehensible explanations to support communication and teaching.

Two such often-related approaches are user-centred design (UCD) and interactive design (IXD); both are concerned with developing systems that are usable. Preece et al. (2015:8) define IXD as "*designing interactive products to support people in their everyday and working lives*". The aim is to design and develop systems that are easy to learn, are effective to use, and provide an enjoyable UX (Preece et al. 2015). UCD places the user at the centre of the process of designing usable products and systems by considering techniques, processes, methods, and procedures in the design process (Rubin & Chisnell 2008). These approaches are at the heart of system development that caters for users' needs and improves usability and UX in interactive information systems.

A principle can be defined as "*a truth or general law that is used as a basis for a theory or system of belief*" (Oxford Dictionary 2018). Preece et al. (2015:25) define design principles as "*generalisable abstractions intended to orient designers towards thinking about different aspects of their designs*". In general, design principles are developed from a combination of theory-based knowledge, common sense, and experience (Preece et al. 2015). There are general design principles for designing information systems, and then there are more specific principles that are meant to accomplish specific design goals. For example, researchers have developed design principles that are meant to achieve usability and UX goals in user interfaces (websites) and other interactive systems. Gould and Lewis

(1985) propose three principles for a computer system to be useful and easy to use. These are widely accepted in the field as key guidelines.

1. **Early focus on users and tasks**

This is a widely accepted principle in all aspects of system design. System requirements need to address the users' needs and, where possible, involve users at every stage of system development. This requires understanding the users from the start by studying their cognitive, behavioural, and attitudinal characteristics, including understanding their mental model of the system (Gould & Lewis 1985).

2. **Empirical measurement**

This involves observing and measuring performance of the intended users using simulations or prototypes and incorporating the performance in the final system. At the beginning of the project, specific usability and UX goals should be identified, clearly documented, and agreed on.

3. **Iterative design**

The design and implementation are iterative, with as much iteration as necessary. This allows problems found in user testing to be fixed, and more tests and observations are carried out to check the effects of the fixes. Preece et al. (2015) provide three key principles for UCD that involve users in the design and development process of a product: (1) technology must be organised around the user's goals, tasks, and abilities; (2) technology should be organised around the way users process information and make decisions; and (3) technology must keep the user in control and aware of the state of the system.

General design principles are applicable to a variety of systems, but as the concept evolved, usability and UX scholars and practitioners have begun to propose more prescriptive design principles for specific types of systems. The more prescriptive design principle studies in the literature include ehealth (Van Gemert-Pijnen, Nijland, Van Limburg, Ossebaard, Kelders, Eysenbach & Seydel 2011), smartphone interface (Mi, Cavuoto, Benson, Smith-Jackson & Nussbaum 2014), gaming UX (Desurvire & Wiberg 2015), user interface (Johnson 2013), and general usable security (Sasse & Flechais 2005). These studies all address the design of specific applications, with little relevance to other categories such as online applications that rely on InfoSec for fulfilling their utility goals.

The wide variety of, and unique nature of, IS applications mean that design principles specifically developed for a particular type of application are almost irrelevant to another category of applications – hence, the need to come up with solutions tailor-made for specific applications. Not many studies have been conducted to address online InfoSec application design, and given the growth of such applications and their reliance on remote authentication, it is critical to come up with solutions that specifically tackle their unique InfoSec challenges. For this reason, this research proposed socio-technical design principles to address the knowledge gap in the design of online InfoSec applications, using online banking as a case study. These design principles were envisaged to be applicable – with minimum adaptation – to other online applications with similar characteristics.

3.7 HUMAN-COMPUTER INTERACTION SECURITY

Human-computer interaction security (HCISec) is a field that deals with aspects in the areas of HCI and InfoSec and is specifically concerned with designing InfoSec systems that are usable. It intends to improve usability of security features in information systems. HCISec is used as an acronym for different terms in the literature, including 'human-computer interaction in security', 'human-computer interaction and security', 'human-computer interaction security', and 'human-computer interaction (security)'. There is generally no consensus on the exact expanded term, and in this research, the researcher uses human-computer interaction security. Regardless, all the above-mentioned terms generally mean the same, that is, HCI as it pertains to InfoSec in end-user applications.

Karat, Brodie, and Karat (2005) identify four unique aspects in HCI design that present challenges and opportunities. Firstly, security is not the main goal of users, and they want it to be transparent and seamless, but still want to be in control of the situation. Secondly, security, which is often designed with highly trained technical users in mind, is now supposed to be used by a totally different type of user, including non-technical novice users. Thirdly, usability is a bigger problem in security, since complexity is at the heart of many InfoSec systems. Lastly, systems must be designed to enable easy and effective updates for continuous protection with minimum user intervention.

Given human memory limitations, most users fail to comply, leading to unsecure behaviour such as sharing passwords, using memorable passwords, or writing down passwords. Sasse and Flechais (2005) argue that, usually, users fail to comply with required security behaviour because it is awkward, not because it is too difficult. For example, insistence on locking computer screens even for brief periods can be construed as hiding something from colleagues in a shared office space (Sasse & Flechais 2005). Human behaviour is generally goal-driven (Payne, Youngcourt & Beaubien 2007); therefore, successful execution of users' tasks is a key aspect of designing successful systems. This calls for InfoSec applications that are goal- and task-driven. This has led to the conclusion that security tasks must be designed to support production tasks, and they must not conflict with production tasks. Hence, there is a need to design systems that have performance requirements for security tasks that are derived from performance of production tasks (Sasse & Flechais 2005).

It is important for users to know that they have a significant role to play in creating a secure environment, and as such, they need to be held accountable for non-compliance. Users must be provided with adequate education and training in the workings of the InfoSec system, with possible actions to be taken against them for non-compliance. Mitnick and Simon (2005) argue that, since social engineering attacks bypass technology, effective security awareness programmes should place the focus beyond the correct usage of security mechanisms by including related behaviour such as verifying callers. Changing user behaviour is a multifaceted task that inherently needs to take a number of aspects into consideration. These include human memory capabilities, user perceptions, organisational and personal goals, and HCI design principles. Therefore, the design of usable InfoSec systems is a task that needs the effort of people from disparate disciplines (Weirich & Sasse 2001).

Computer security is complex enough, and adding users makes it even more problematic (Schneier 2000). An InfoSec system that is not user-friendly fails in the marketplace, or users evade the security features or, worse, avoid using the whole system altogether. Unfortunately, usability problems with InfoSec systems go beyond just user interfaces and require a wider application of HCI concepts and design approaches (Flechais, Mascolo & Sasse 2007). The inherent human problem in information security gave rise to the notion of usable security, which strive to make information security mechanisms usable to the intended users.

3.8 USABLE SECURITY

InfoSec is challenging to the usability community, mainly because of the principle of security through obscurity that has existed in the security environment for far too long. It dates back to the early days of encryption algorithms, where secret keys were the norm. The use of secret keys has since proven to be ineffective in solving InfoSec problems, especially in this networked environment that relies on remote authentication for granting access to services. Regardless, security is often complex, making it difficult to understand and easy to misconfigure and misuse. This is aggravated by the fact that users are usually not motivated to apply more effort to security when completing production tasks (Payne et al. 2007). Consequently, HCI and human factor aspects of InfoSec have come to the fore, with great interest in design principles that allow users to use InfoSec mechanisms effectively in applications.

There have been usable security studies in a number of areas, including ehealth (Yeratziotis et al. 2012), email encryption (Hof 2013), smart buildings (Bo, Zhang, Hong, Sun & Huang 2014), and online banking authentication (Althobaiti & Mayhew 2014). Within the same area, different usable security studies may concentrate on a specific issue of the systems such as design principles, system authentication, and the user interface. All of these approaches have a single goal of designing and developing systems that exhibit usable security characteristics that provide effective security to the user, while being usable. Therefore, this research proposed a socio-technical framework for the development of secure and usable online banking systems.

Generally, computer users expect computers to perform certain ‘magical’ actions. Thus, it is essential that security and usability be complementary rather than have contradictory goals. Secure systems are more manageable, more dependable, and, ultimately, more usable. Basically, both security and usability require that the computer should satisfy the user’s needs and wants, no more and no less (Yee 2004a). One of the earliest landmark studies on usable security was the work of Whitten and Tygar (1999), which evaluated the usability of PGP 5.0 in email encryption. The authors define usable security based on a set of four priorities:

> “*Security software is usable if the people who are expected to use it: (1) are reliably made aware of the security tasks they need to perform; (2) are able to figure out how to successfully perform those tasks; (3) don’t make dangerous errors; and (4)*

> *are sufficiently comfortable with the interface to continue using it*" (Whitten & Tygar 1999:170).

The integration of security properties in the user interface design has inherent problems that design strategies need to address. Whitten and Tygar (1999) identify the following five such problematic properties:

1. The unmotivated user property

Users are generally unmotivated to perform security tasks, as these are viewed as being in the way of achieving production tasks. Security is usually a secondary goal; therefore, security tasks need to be seamless. For example, for a user whose primary goal is to make a payment using online banking, it is natural to put off learning about a secure connection or to just be optimistic and assume that his/her security is working. InfoSec designers of user interfaces should come up with security designs that are seamless and unobtrusive, as users will avoid security mechanisms if they find them too difficult or annoying.

2. The abstraction property

InfoSec management often involves security policies that provides access control rules to resources. The creation and management of such rules need careful attention to avoid alienating users from a wider population and the design of user interfaces need to consider this property.

3. The lack of feedback property

Applications need to provide good feedback to the user to prevent dangerous errors but it is difficult to provide good feedback for security applications. Given the complex nature of security configuration, any attempts to summarise are usually inadequate. Moreover, only users really know what they want, making it difficult for InfoSec software to perform adequate error checking. To make matters worse, too much feedback to the user can be exploited by attackers to learn system properties that enable successful attacks. For instance, informing the user exactly which of the supplied credentials (between a username and a password) is incorrect assists the brute-force attacker.

4. The barn door property

This property states that once information assets are left unprotected, even for short period of time, there is no way to know if it has not yet been compromised. Hence, it is important for user interface design to place high priority in assisting users to avoid making high risk mistakes.

5. The weakest link property

Security in a networked environment is as strong as the weakest link in the security chain. Hence, attackers only need to exploit a single component and the security of the whole system is compromised. As such, users need to be assisted throughout all steps of securing the system and avoid random exploration.

These properties are still relevant, as shown by recent personal information records breaches, which are often discovered years after the breach has taken place. A good example is the security breach at Yahoo that compromised all three billion user accounts in 2013, but was only discovered and reported on in 2016 (Fiegerman 2017, Perlroth 2017). Hackers often access computer systems and steal and sell personal information without detection for long periods of time. The STInfoSec framework, by using the socio-technical approach, was essentially aimed at mitigating the threats of humans (users) as potentially the weakest link. This was achieved by developing design principles accompanied with checklist items that exhibited usable security properties in the STInfoSec framework.

3.8.1 Usable security principles

A great deal of research has been conducted on the design guidelines that are meant to improve security-oriented design. Generally, there is no consensus on exactly what makes one design better than another from a usable security perspective. Since security and usability are often traded off against each other, the intricacy and overheads of security solutions are often obstacles to their effective and efficient deployment (Dourish & Redmiles 2002). In addition, despite the technological advances that have created impressive technical InfoSec systems (Choo 2011b), technology does not solve all security problems (Schneier 2000). Achieving this balance has been a challenge, and while much research on both usability and security has been conducted, there is little on the topic of usable security. The need to address not only functional aspects of InfoSec systems, but also system usability, makes such systems effectively socio-technical systems (STS), as they bring together ideas from different areas to address a common problem. Usable security draws from the fields of InfoSec, usability, and user behaviour in interaction with computer systems.

This section discusses design guidelines and principles meant to improve the design of InfoSec systems. There is an overlap with some of the usability principles already mentioned in section 3.3 those already mentioned are not repeated here. Several researchers have developed and proposed usable security design guidelines and principles. Only the guidelines and principles most relevant to the system currently under investigation are discussed here.

Studies by Yee (2004b; 2002) are among the earliest that have gained significant recognition in the design of usable security. Yee proposes addressing valid and non-trivial issues specific to usable security design by developing a list of 10 principles:
Path of least resistance – provide the most comfortable way to complete tasks by granting the least authority.
Explicit authorisation – a user's authorities should only be provided to other actors after obtaining explicit authority for such granting.
Revocability – users should be able to revoke serious errors, and the system should give prior warning and confirmation for irreversible actions. Provide support for 'undo' and 'redo' functions.
Visibility – keep users informed about the system security status, using appropriate feedback within a reasonable time.
Expected ability – the interface must not give the user the impression of having authorities that the user does not actually have.
Trusted path – protect the user's communication channels against man-in-the-middle attacks that manipulate authority on the user's behalf.
Expressiveness – enable the user to express safe security policies in terms that fit the user's task. Guide users through security features, and allow freedom of expression.
Appropriate boundaries – draw distinctions among objects and actions along boundaries relevant to the task.
Identifiability – present objects and actions using distinguishable, truthful appearances.
Clarity – clearly indicate the consequences of actions and decisions that the user is expected to make.

In addition to the above, other authors have proposed a number of usable security principles that address both InfoSec and usability in ISs. These are discussed below and include only those under investigation in this research:

Availability – system services must be available all the time, with minimum downtime.

Help and documentation – these must provide user assistance, with searchable help and documentation for both security and non-security tasks that is actionable with concrete steps.

User suitability – the system should provide options suitable for users with diverse levels of skill and experience in security.

User language – the system should speak the users' language, with words, phrases, and concepts familiar to users, rather than system-oriented terms.

Security – ensure end-to-end protection of the communication channel between the end-user device and trusted servers.

Privacy – protect the information provided by users against access by unauthorised parties, and use it only for the purposes for which it was collected.

Based on Yee (2004b), the STInfoSec framework (the product of this research) suggests usable security design principles, accompanied by checklist items for each principle. The principles satisfy usable security properties for online InfoSec applications, and to ensure validity, the framework principles were evaluated using a heuristic evaluation method.

3.8.2 Online banking authentication

Online banking websites and applications, like any other online and offline information systems, rely heavily on passwords and PINs for authentication. There are numerous weaknesses in this kind of authentication, such as the password requirement of precise character recall, especially given that precise recall is not a strong point of the human intellect. Cyberattacks attempt to obtain users' login credentials through sophisticated malware and keylogging. There is usually a trade-off between having a complex password that is difficult to crack, on the one hand, but easy enough to remember, on the other. Password-cracking is easy, given a determined attacker, especially now that computing power is easily available to perform brute-force attacks. Banks worldwide use a multitude of credential combinations for online banking login, all with the aim of improving system security.

South African banks require credential information consisting of either a username, email address, profile number (user ID), or account number/card number, and any combination of these pieces of information. The next piece of authentication information is the verification of either the password or PIN, or both. Some banks provide partial password characters that the user has to complete by supplying the missing characters to complete the authentication process. Such a mechanism improves the usability of the system with regard to password memory, but might expose the system to attacks by an assailant collecting password characters on different attempts. Other protections exist, which include locking the user out after a number of failed attempts. Users are usually allowed to change passwords and PINs online at any time, but there is no policy to force periodic password changes.

Internationally, the Bank of America, Credit Suisse, and Citibank are among those banks that use a combination of user ID and password for online banking. Some banks such as the HSBC (UK and USA) and Barclays Bank UK improve the security of the system slightly by not providing the details of all the required login credentials needed on the online banking login webpage. That is, the user needs to provide a valid user ID first before revealing exactly what the next piece of login information is. This provides an added level of security, especially against brute-force attacks.

For a more advanced online banking system, numerous international banks use various security token devices that generate regular token codes to be entered online. These include JPMorgan Chase, which gives users the option of improving security by requesting a token device. BNP Paribas uses a more complex process, with multiple stages and credentials that include a hardware token device to access online banking. Initially, the user provides the user number/customer number and the card number. Then, the user inserts a bank card into the token device and enters a website-generated eight-digit number, followed by the bank card PIN. Finally, an electronic signature is generated by the token, and this is entered on the website to complete the login process.

It is interesting to note that banks worldwide have not agreed on a single secure online banking login process. The existence of these different online banking login processes highlights the lack of consensus on a single universal login process that is regarded as secure by banking organisations. A variety of online banking login systems exist worldwide that offer different levels of security. Banks are still experimenting with different systems and often use the level of security provided as a competitive advantage in the industry. This leaves users of certain banks vulnerable to a variety of sophisticated online attacks. Nevertheless, there is some cooperation in combating cybercrime, with consortiums that share information on the latest security risks and ways to avoid security breaches. The consortiums also run client awareness programmes to educate users on InfoSec risks.

There are numerous online InfoSec threats faced by organisations and individuals that conduct daily online activities. As such, technical solutions alone are not sufficient to protect information assets at risk from adversaries. Hence, this research proposes the STInfoSec framework that encourage equal treatment of social and technical aspects in online InfoSec application design and development.

3.9 THEORETICAL FRAMEWORK

This section explains the concepts relevant to this research as presented in the theoretical framework, giving insight into how data was collected on the relevant concepts and their subsequent analysis. It also identifies significant factors, variables, and relationships among items to provide a theoretical overview for the design of secure and usable online InfoSec applications. The conceptualisation helped to identify key InfoSec design principles applicable to online InfoSec applications as provided in section 3.10 that outlines the preliminary framework. The conceptualised principles, in turn, guided the data collection and assisted in answering the research questions posed in this research. Many factors influence the adoption and continued use of online banking, ranging from users' mental models of the system to intrinsic design nuances.

The synergy of these building blocks is important in delivering online banking that is secure and gives the user an overall satisfactory experience. Therefore, it was critical to consider all aspects of the process, from user attitude and behaviour towards InfoSec systems to design approaches that are user-centred. To recap, the main objective of this research was **to develop a socio-technical framework that assist in the development of secure and usable sensitive online applications**. The following sections conceptualise the survey items for quantitative data collection constructs based on UTAUT2 and usable security that consists of the intersection of usability and security.

3.9.1 Unified theory of acceptance and use of technology

As mentioned in Chapter 4, the main theoretical foundation of this research was UTAUT2, especially with regard to how security and usability aspects affected acceptance and continued use of technology, using online banking as a case study. UTAUT2 unifies eight disparate theories or models of user information technology acceptance and use, thereby streamlining the determinants of information technology adoption and continued use. Hence, UTAUT2 covers a wide range of constructs to model user interaction with information systems. Section 3.9.3 further on in this chapter outlines the hypotheses based on the constructs.

The current version, UTAUT2, incorporates additional constructs that influence behavioural intention and use behaviour. In this research, use behaviour was measured by use frequency. The researcher investigated key constructs, namely, performance expectancy, effort expectancy, social influence, hedonic motivation, facilitating conditions, price value, and habit as direct or indirect determinants of acceptance, adoption, and continued use of online banking. Gender, age, experience, income, education, ethnicity, device, and use frequency were hypothesised to moderate the effect of the constructs on adoption and behavioural intention.

3.9.2 Usable security

The investigation of usable security incorporated both security and usability principles. For quantitative data collection from online banking users, six usability constructs were considered, while security consisted of 13 survey items that covered both security and privacy issues. The concepts under investigation pertaining to usability included learnability, user suitability, satisfaction, availability, errors, and help and documentation. These were again moderated by the same moderating factors mentioned under the UTAUT section above. Also included in usability assessment were the 10 items of the system usability scale (SUS) measurement tool. Of the 13 survey items concerning security and privacy, six items related to security and seven to privacy. The survey is provided as Appendix E.

3.9.3 Development of hypotheses

This section outlines the hypotheses developed and tested through the survey data based on the underlying constructs of the theoretical framework. The constructs of the model are first explained briefly, and the main research hypotheses associated with the constructs are listed. The broader research hypothesis postulated that **'socio-technical aspects of system design enhance the adoption and continued use of information security applications'**. Therefore, the research hypothesised that constructs from UTAUT2, usability, and security had an effect on the adoption and intention to use online banking. The definitions of some of the UTAUT2 constructs were first provided in the original UTAUT and the eight unified models; these definitions are still relevant in the second version of the model. The effect of the constructs on adoption and continued use of online banking was moderated by a number of factors, which included gender, age, experience, education, employment, income, ethnicity, and device. The data analysis determined which of these moderating factors had a statistically significant impact on the constructs under investigation.

Performance expectancy

Performance expectancy (PE) is the degree to which an individual believes that using the system enhances activity performance (Venkatesh et al. 2003). PE was first defined in UTAUT and is a derivative of five constructs from the different models unified in UTAUT. It is the strongest predictor of intention and remains significant at all points of measurement in both voluntary and mandatory settings (Venkatesh et al. 2003).

H1: **Performance expectancy** has a positive and significant impact on individual **behavioural intention** to use online banking services.

Effort expectancy

Effort expectancy (EE) is the degree of ease associated with the use of the system and is a derivative of three constructs from the unified models, namely, perceived ease of use, complexity, and ease of use (Venkatesh et al. 2003).

H2: **Effort expectancy** has a positive and significant impact on **behavioural intention** to use online banking services.

Social influence

Social influence (SI) is the degree to which an individual perceives that other people believe he or she should use an information system, as it determines behavioural intention, and is a derivative of subjective norms, social factors, and image (Venkatesh et al. 2003).

H3: **Social influences** have a positive and significant impact on an individual's **behavioural intention** to use online banking services.

Facilitating conditions

Facilitating conditions (FC) refers to the degree an individual believes that organisational and technical infrastructure exists to support the use of the system (Venkatesh et al. 2003). The researcher investigated the effects on intention to use online banking based on access to resources such as internet connection to, and assistance in, using the service.

H4: **Facilitating conditions** have a positive and significant influence on **behavioural intention** to use online banking services.

Hedonic motivation

Hedonic motivation (HM) is the enjoyment of using a system, which plays a significant part in influencing technology acceptance and continued use (Brown & Venkatesh 2005). HM complements UTAUT's strongest predictor, that is, performance expectancy, which emphasises usefulness (Venkatesh et al. 2012).

H5: **Hedonic motivation** has a positive and significant impact on an individual's **behavioural intention** to use online banking services.

Price value

Price value (PV) is the consumer's awareness of the trade-off between the perceived benefits of the application and the monetary cost of using the application (Dodds, Monroe & Grewal 1991). The cost of using a system is significant in a consumer context compared to an organisational context where employees do not bear such costs. Hence, the introduction of PV in UTAUT2 has a significant influence on the adoption and continued use of the system from an individual perspective (Venkatesh et al. 2012).

H6: **Price value** has a positive and significant impact on **behavioural intention** to use online banking services.

Habit

Habit (H) is the extent to which people tend to perform behaviours spontaneously due to learning (Limayem, Hirt & Cheung 2007). As an additional construct in UTAUT2, habit is related to experience in system use based on the duration from first use (Venkatesh et al. 2012).

H7: **Habit** has a positive influence on **behavioural intention** to use online banking services.

Behavioural intention

Behavioural intention (BI) is an individual's perceived likelihood to engage in a given behaviour (Ajzen 1991). Venkatesh et al. (2003) theorise that behavioural intention has a significant positive influence on technology usage. In addition, the researcher theorised that user intention to use technology depended on the effort involved in using the technology.

H8: **Behavioural intention** has a positive and significant impact on **effort expectancy**.

H9: **Behavioural intention** has a significant positive influence on **use behaviour (use frequency)**.

Security

Security (S) and, specifically, perceived security risk have been found to have a significant impact on online consumer behaviour. Given the potential of financial loss, the security risk does not have to be real for the behaviour of consumers to be affected negatively regarding intentions to use an online service (Chiu, Wang, Fang & Huang 2014).

H10: **Security** has a negative and significant impact on **behavioural intention** to use online banking service.

Privacy

Privacy (P), in the context of an online environment, has to do with protection of consumers' personal information against unauthorised access and subsequent use. Given the prevalence of attacks that rely on personal information, such as identity theft, the system should be able to protect users' personal information.

H11: System **privacy** has a negative and significant impact on **behavioural intention** to use online banking services.

Usability

Usability is measured by six constructs: learnability, user suitability, satisfaction, availability, errors, and help and documentation. In addition, the survey instrument included a 10-item SUS measurement tool. The overall usability hypothesis is as follows:

H12: System **usability** has a positive and significant impact on **behavioural intention** to use online banking services.

Moderating factors

UTAUT2 has three moderators, namely, age, gender, and experience. In addition to these, this research postulated six additional moderators: income, education, ethnicity, device, use frequency, and bank. Although data was collected on all these moderating factors, the analysis did not include or mention bank names for ethical reasons and avoid prejudice. The moderating factors were not mentioned explicitly in the hypotheses, but their effects on model constructs were investigated and reported separately and incorporated in the final structural model.

3.10 PRELIMINARY STINFOSEC FRAMEWORK

This section outlines the proposed STInfoSec framework that drew from the literature on usable security design principles and best practices. The end result was a set of critically informed design guidelines for online InfoSec applications such as online banking. In the final framework, the design principles were validated through a heuristic evaluation method. The four STS components are first explained in the context of online banking, describing what constitutes each component. The framework proposed in this research integrated UTAUT2, usability, and security in a socio-technical system in the design and development of online applications.

Until recently, InfoSec practitioners were only skilled in technical aspects of protecting information assets, with usability and human factors being an afterthought. This created a gap between InfoSec and usability – hence, the need for integration in addressing the InfoSec problem, given that users have since been identified as the weakest link in the InfoSec chain. Combined with UTAUT, STS can be used to investigate user acceptance and continued use of technology. UTAUT essentially predicts users' behaviour in deciding to adopt or reject a technology artefact. Thus, aiding the development of such artefacts through improving aspects that significantly make users reject a technology, such as lack of usability and security, while optimising positive aspects, helps improve the adoption and continued use of such technology.

3.10.1 STInfoSec components

This section outlines the building blocks of the STInfoSec framework drawn from the literature on usable security design principles and best practices. The end result was critically informed design guidelines for online InfoSec applications such as online banking. In the final framework, the design principles were validated through a heuristic evaluation method.

In this part, the researcher first explains the four STS components in the context of online banking, describing what constituted each component. The following section discusses individual framework components. The STInfoSec framework looked at improving the development of online applications that relied on effective InfoSec to provide services to the user. The idea was to make these applications meet both usability and security requirements, thereby creating an environment that would foster adoption and continued use of the applications by a diverse set of users. The framework specifically applies to online banking systems, but can be applied to any other online security IS application, with minimum adaptation. Figure 3-4 illustrates the framework components, including external elements that contribute to the framework.

Secondly, usability and security requirements are presented that are necessary for secure and usable InfoSec applications. These are design principles that developers need to address in developing applications that meet usable security properties. In the third place, using UTAUT2, the investigation into users' perceptions of the current online banking service is provided, highlighting areas that need attention to improve the service based on user feedback.

Usability

Usability plays an important role in facilitating effective and efficient use of the system, and it has a significant impact on potential users' adoption and use of the system. Therefore, it is essential that information systems implement usability principles from the outset when design decisions are made, as usability cannot be an add-on component at a later stage. There is significant research on the usability principles that need to be addressed in developing IS applications, as explained in previous sections. Some of these are general guidelines, while others have been developed for specific types of applications. In this study, the interest was usability principles intended for InfoSec applications, that is, principles for usable security.

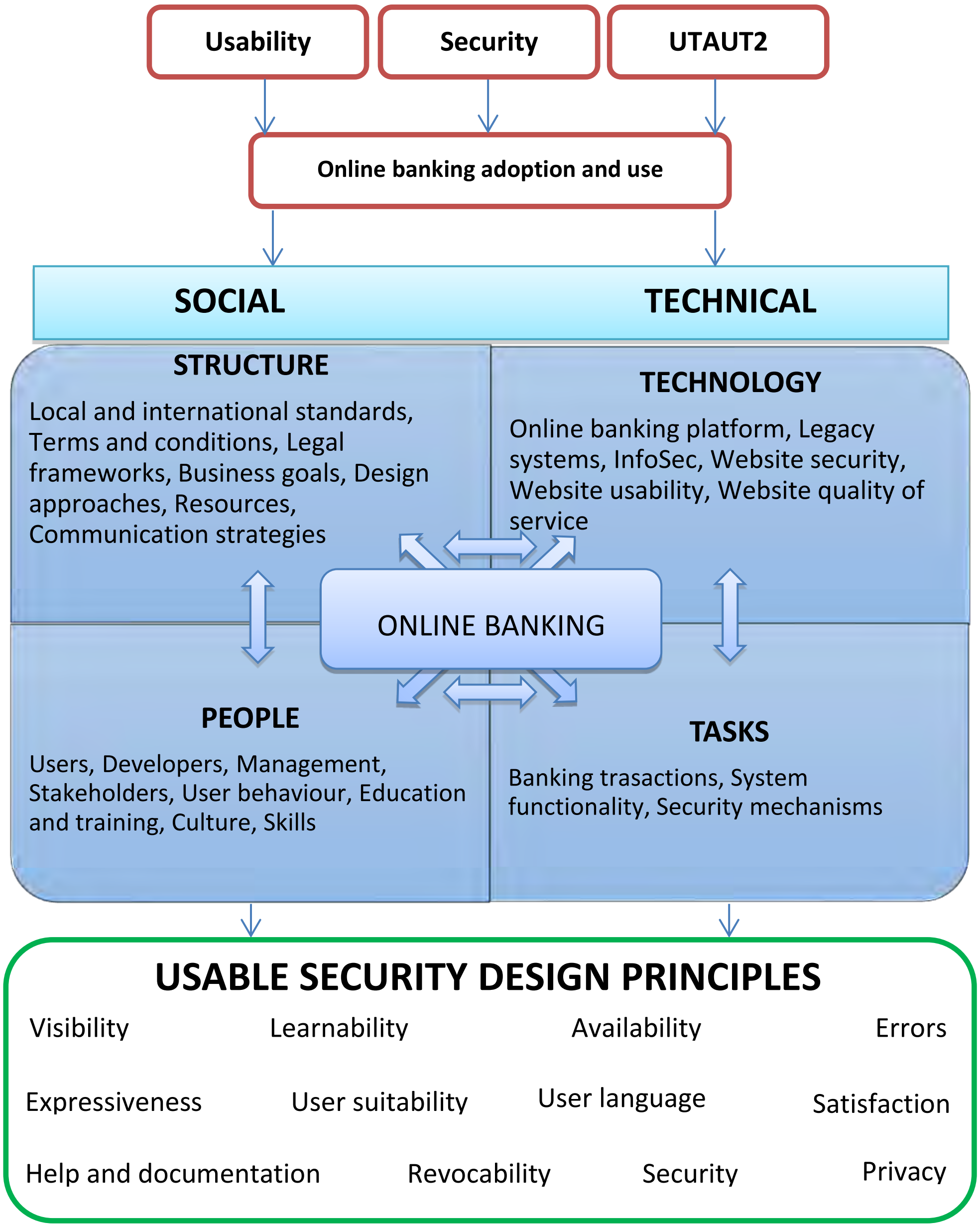

Usability
Security
UTAUT2
Online banking adoption and use
SOCIAL
TECHNICAL
STRUCTURE
Local and international standards, Terms and conditions, Legal frameworks, Business goals, Design approaches, Resources, Communication strategies
TECHNOLOGY
Online banking platform, Legacy systems, InfoSec, Website security, Website usability, Website quality of service
ONLINE BANKING
PEOPLE
Users, Developers, Management, Stakeholders, User behaviour, Education and training, Culture, Skills
TASKS
Banking trasactions, System functionality, Security mechanisms
USABLE SECURITY DESIGN PRINCIPLES
Visibility
Learnability
Availability
Errors
Expressiveness
User suitability
User language
Satisfaction
Help and documentation
Revocability
Security
Privacy

Figure 3-4: STInfoSec framework components

Security

Information system applications need to protect confidential and sensitive information provided by users for the system to be trusted. This protection of information requirement is particularly important when the risk includes potential financial loss and leaking of private information that can lead to identity theft. One such system is the online banking system. The security or perceived security of an online banking system, as viewed by users, needs to be trustworthy for them to adopt or continue to use the service. Hence, the design of the system needs to address security mechanisms to protect users' personal information. Several design principles for the development of a secure IS were found in the literature.

UTAUT2 model

Sensitive online applications such as online banking need more than just usefulness and ease of use to encourage potential users to adopt them. Usability, security, privacy, and trust, be these perceived or real, need to be addressed for users to be comfortable with adopting and continuing to use the systems. With the advent of more pervasive mobile and portable devices, the emphasis has moved to addressing UX when users interact with these devices. In this research, it was found that users and developers of online banking applications raised both social and technical issues regarding InfoSec. Therefore, the design of such applications needs to address both aspects as well.

Socio-technical components

Studies of the socio-technical approach to InfoSec are mainly based on technical and organisational aspects of system design, which are the main foundation of the socio-technical model. This research addressed socio-technical aspects based on individual context, rather than an organisational setting. The main objective of the STInfoSec framework was to gain a better understanding of how socio-technical aspects that affected InfoSec usage could assist in the development of online applications in the context of online banking. The specific technical and social dynamics at play in users' interaction with InfoSec mechanisms have been widely researched separately. This research intended to bring these dynamics together in the context of usable security.

Theoretically, InfoSec elements in an IS can be classified according to three categories: social, technical, and socio-technical (Iivari & Hirschheim 1996). Social and technical views place emphasis on either social or technical aspects, respectively, while a socio-technical view appreciates social and technical aspects of information system development equally. As a system, socio-technical systems strive to encourage a systems approach, with a holistic approach to IS development that addresses InfoSec problems brought about by the interrelationship between users and technology. Rather than approaching the two aspects separately, the emphasis is on approaching the social and technical components of the system simultaneously. Ropohl (1999) argues that a socio-technical systems model is useful in explaining the impact of technology on society, making technical development equivalent to social change. The following subsections discuss the four components of STS in the context of online banking.

Structure

The structure component deals with policy and legal elements that ensure a code of conduct among different groups of people involved in the system. Financial institutions are governed by a country's rules and regulations regarding the provision of financial services to its citizens, usually through the country's central bank and other financial regulatory bodies. The banks, in turn, create banking and online banking terms and conditions that set recommended behaviour for users, including responsibilities and liabilities that accompany registration and continued use of the services provided. These terms and conditions include dispute resolution procedures in case of security breaches or other related disputes, which are usually referred to the banking ombudsman when the parties (the user and the bank) fail to resolve the issue.

Structure also includes design approaches used in developing the system, including local and international standards and best practices that are compulsory or recommended in application (or product) design and development. Such standards might include those prescribed by international bodies such as the ISO and national bodies such as the South African Bureau of Standards (SABS), as well as other InfoSec recommendations from local and international banking consortiums. Most South African banks are members of SABRIC, a non-profit company formed by the four major South African banks to assist banking and cash-in-transit companies in combating organised bank-related crimes (SABRIC 2018). SABRIC provides a platform for financial institutions to share information on InfoSec and security threats. Communication strategies are part of this component. These include the preferred means of communication as selected by the user during registration for services such as online banking.

People

The people involved in an online banking system include users, developers, management, and any other stakeholders such as vendors, contractors, etc. Users are the bank's clientele – a diverse group of people with different ages, educational qualifications, computer literacy levels, incomes, languages, and cultures. 'Developers' is an all-encompassing term that includes designers, programmers, testers, usability evaluators, vendors of outsourced products, and any other people directly involved in the development of online banking applications. Management includes top management of the financial institution and the supervisors of the development teams. Those in top management have direct influence on the development of the system, as they make decisions that directly affect the end product, such as controlling the budget and hiring personnel with relevant and needed expertise to improve the final product.

Technology

The technology component involves a wide range of technologies that form part of the online banking system – from the bank's hardware and users' devices to the software applications that provide the services. From the bank's side, the technology covers hardware servers, operating systems, networking technologies among data centres, middleware platforms, back-end applications, and the user interfaces that allow employees and users to access information remotely. The bank also provides InfoSec technologies and mechanisms to protect users and company information assets by providing access to authorised users based on predefined access control policies. Such technologies include encryption, firewalls, and intrusion detection and prevention systems. User interfaces for both the web and mobile devices need to incorporate current best practices to enhance user-friendly properties, which include acceptable usability, and to enhance UX. Given the wide range of activities currently accessible through the internet, including games and entertainment, online applications must be competitive for users to embrace and use them.

Tasks

The structure and technology in a socio-technical system provide the means for people to accomplish certain tasks. An online banking system provides a convenient way for the bank to offer banking activities to its clients 24 hours a day. Apart from an array of online banking transactions, the system must also fulfil the organisational business goals to provide the shareholders with a return on their investment. Users perform banking-related tasks, and the development team, thus, ensures that the online banking system is readily available to users and that it is usable and secure to meet users' expectations and fulfil business goals.

3.10.2 Usable security principles

A large volume of research has been done on design guidelines that are intended to improve security-oriented design. Generally, there is no consensus on exactly what makes one design better than another from a usable security perspective. This section discusses design guidelines that are meant to improve user interface design of IS applications, particularly those that require InfoSec mechanisms. Several researchers have investigated usable security design strategies. Among the earliest studies are those done by Shneiderman et al. (2016), Yee (2004b), (Johnston et al. 2003), and Nielsen (1995). These researchers identified a gap between usability and security, and to bridge this gap, they came up with numerous design principles, some of which were generic for any kind of application, while others were application-specific. In this regard and for this research, the researcher maps themes from qualitative interview data and usable security principles from literature, survey, and interview. The section below describes the principles and outlines the source of each principle as well as the motivation for its inclusion in the research framework.

Principle 1: Visibility

Visibility of the system status to let users know exactly what the capabilities of the system are, is one of the most important principles addressed by both usability and usable security scholars. Nielsen (1995) mentions it as a criterion for usability evaluation of the user interface, while Katsabas, Furnell, and Dowland (2005), Yee (2004b), and Yeratziotis et al. (2012) emphasise the principle in the context of usable security in order to let users know whether an application or user interface is using any protection mechanisms. Hence, applications such as web browsers now display the ‘lock’ icon on ‘https’-protected web-sites. The importance of visibility is implicit in usable security. Therefore, the researcher did not deem it necessary to directly investigate its significance; as such, the principle was included indirectly from the literature and as part of the security principles.

Principle 2: Learnability

The ability of users to efficiently and effectively use an application or user interface for the first time, as well as subsequent reuse, depends on the ease of learning the system (Preece et al. 2015). As such, learnability has been identified as an essential component in the definition of usability (Nielsen 2010). The importance of users’ ability to consistently use InfoSec mechanisms all the time cannot be overemphasised. Hence, learnability is an essential part of creating a secure environment, and applications need to address this principle to assist users to remember how to use the system on their return (Yeratziotis et al. 2012). The principle was addressed in both the user survey and interviews with developers under the section on training and education.

Principle 3: Satisfaction

Satisfaction was included as a principle under the usability section of the survey and the hedonic motivation construct in UTAUT2. Satisfaction is one of the five characteristics of usability identified by Nielsen (2010). Essentially, satisfaction in the use of a system extends beyond usability and into the realm of UX (Bevan 2008). User satisfaction is influenced by UX (Deng, Turner, Gehling & Prince 2010) through such aspects as social presence (Ogara, Koh & Prybutok 2014). Hedonic motivations encourage users to engage with a system, influencing the overall UX, which is a direct enabler of user satisfaction (Zahidi, Lim & Woods 2014, O'Brien 2010).

Principle 4: Errors

The principle of errors, be it for their prevention in the first place or recovery after they have occurred, is a critical design principle in all systems. Therefore, this principle is important in both usability and InfoSec design strategies. Nielsen (1995) includes two usability principles that address error-related usability problems, namely, *error prevention* and *help users recognize, diagnose, and recover from errors*, while Shneiderman et al. (2016) suggest that user interface design should offer simple error handling to users as one of the 10 golden rules. Error handling is important in usable security to avoid critical mistakes and disclosure of sensitive and confidential digital information assets (Katsabas et al. 2005). This principle was addressed in the user survey to ascertain the prevalence of errors and the effectiveness of error recovery mechanisms.

Principle 5: Availability

Availability is essential for online applications, which are often marketed as providing convenience by allowing users to access a service 24 hours a day. In the real world, a certain period of system downtime is expected for reasons such as system upgrades and maintenance, but these activities should be scheduled during off-peak times and kept to a minimum in terms of the frequency and duration of downtime. Yeratziotis et al. (2012), for example, suggest that usable security design should make sure that system services are available all the time, with minimum downtime. In this research, the principle of availability was addressed in the user survey as a construct under usability, and users also raised availability as a concern in the qualitative section of the survey. (See section 6.3.3.)

Principle 6: Revocability

Users should be able to undo actions and errors, and a secure and usable system should give prior warning and confirmation of actions that are irreversible. Although some actions cannot be reversed after a certain stage of processing, developers need to try, by all means possible, to provide support for 'undo' and 'redo' functions. This principle is one of the 10 golden rules of user interface design identified by Shneiderman et al. (2016) and Yeratziotis et al. (2012) as necessary in usable security design.

Principle 7: Expressiveness

The system should inform and guide users through security features and yet allow freedom of expression. The system's InfoSec policy must not be too rigid and difficult for users to comply with; it should, for example, prescribe safe passwords, but still allow users the freedom to create passwords they can easily remember (Yee 2004b). This, in turn, eliminates the need for writing down passwords, which might be necessary if the system has password requirements that are too complex. Security features of integrity and confidentiality are available on most e-commerce web sites. One of the ways in which these features are implemented is through SSL. Johnston et al. (2003) refer to this principle as conveying security features, where the system needs to inform the user in a clear manner of the available security features.

Principle 8: User language

User language is another principle that is relevant in both the usability and usable security contexts. The principle requires the system to speak the users' language, using terms and concepts familiar to users, while avoiding the use of technical terms (Nielsen 1995). This decreases the chances of users making mistakes or misunderstanding system commands. The principle was investigated in the survey.

Principle 9: User suitability

User suitability ensures that the system provides options suitable for users with diverse levels of skill and experience in security (Yeratziotis et al. 2012). Personalisation and customisation of the system are essential for user suitability and allow users to set up preferences that make it comfortable for them to use the system effectively. Although user suitability did not pass the model of fitness test for inclusion in the final structural model, as a principle it was included based on its significance in the literature in the context of usable security.

Principle 10: Help and documentation

Users may need assistance, especially for applications that have been developed for a diverse group of users with different levels of skill. Support material that helps new users and system documentation for reference during usage are critical. Such material must be complete, consistent, correct, and usable for it to meet its intended goals. The principle of help and documentation is generic and is essential for all kinds of systems, products, or services. For online applications, the system needs to provide searchable help and documentation for both security and non-security tasks that are actionable with concrete steps (Shneiderman et al. 2016). This principle was included in both the survey and interviews.

Principle 11: Security

The system should ensure a trusted path through the communication channel (usually the internet) between the end-user device and trusted servers, addressing fundamental InfoSec principles such as confidentiality, integrity, and availability, to avoid disclosure and unauthorised access of information assets in storage and in transit. Ensuring the usability of an InfoSec system should not mean a compromise in the technical functionalities of the system to protect information assets. The security principle was addressed in the survey as a construct and was raised by respondents in the qualitative part of the survey, while it also came up on numerous occasions during interview sessions.

Principle 12: Privacy

Organisations collect personal information about their customers, some of which is sensitive, such as credit card numbers. Hence, the system should protect information provided by users against access by unauthorised parties, and it should be used only for the purposes for which it was collected in the first place. Unfortunately, organisations still have some way to go in improving protection of personal information, with an increasing number of high-profile privacy breaches. The researcher investigated the principle in both the survey and interviews.

3.11 CHAPTER CONCLUSION

The chapter presented the second part of the literature review, with the objective of providing a detailed critical discussion of usability and design principles. The chapter outlined the social component of the socio-technical approach to information security. HCI has come a long way, and several studies have been conducted on different aspects of HCI, which include human factors, ergonomics, and usability. Usability in the context of usable security enables the development of applications that have security mechanisms that users can effectively use. Researchers have developed numerous design principles; some are meant for general applications, while others have been developed for specific applications. Furthermore, certain usable security design principles have been developed for general applications and others for specific applications.

Website usability is critical to achieving usable security in online InfoSec applications, as it forms part of the delivery channel of these applications. Consequently, any in-roads made in designing these applications can be eroded by poor website usability that might frustrate the end-users and have a negative impact on the adoption of the services offered. Online banking authentication forms an integral part of protecting sensitive personal user information. Hence, any design approach to address online InfoSec problems needs to take possible challenges pertinent to the authentication process into account. The goal is to provide remote authentication mechanisms that are usable, so that users do not attempt to bypass them. The theoretical framework includes three aspects: UTAUT2, usability, and security. These informed the design principles included in the preliminary STInfoSec framework. The 12 usable security design principles forming part of the STInfoSec framework are discussed next.

Chapter 4 provides a detailed discussion of the research design and methodology that the research applied in answering research questions and in pursuit of research objectives. The chapter essentially outlines the roadmap of the entire research project.

-- oOo --

CHAPTER 4 RESEARCH DESIGN AND METHODOLOGY

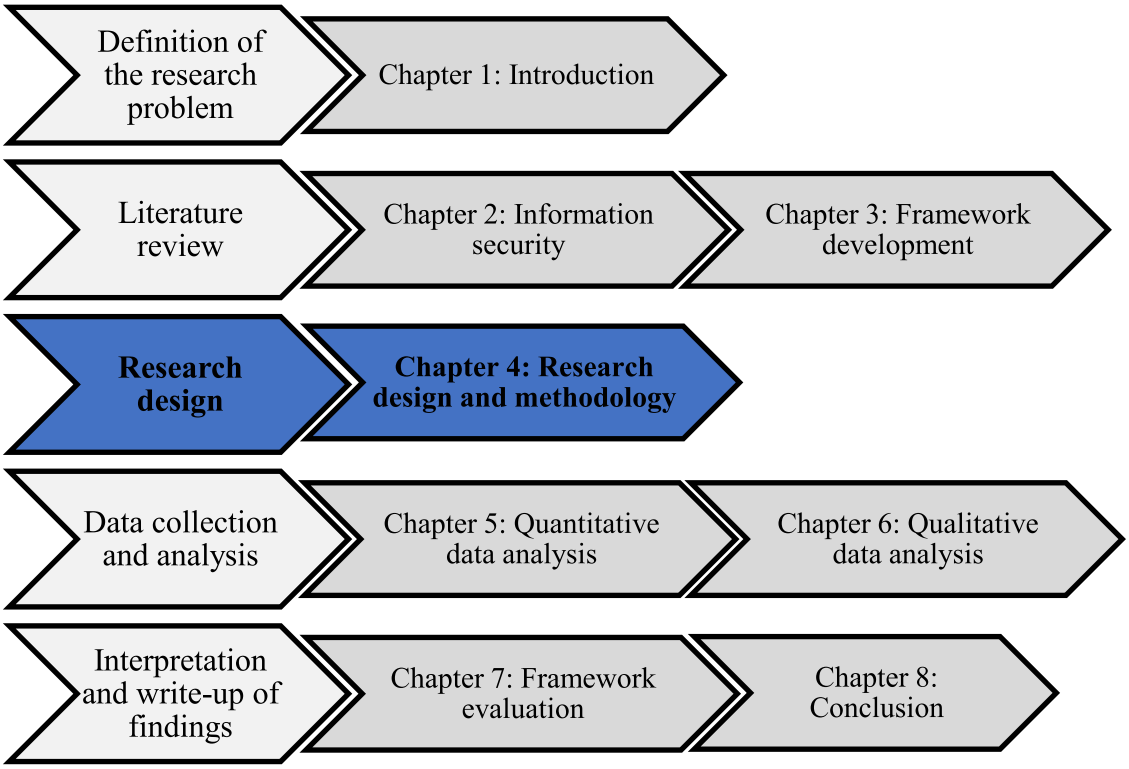

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 4-1: The research roadmap

4.1 INTRODUCTION

The main purpose of this research was to develop a socio-technical framework (STInfoSec) for the design of online InfoSec applications. The proposed framework brought various InfoSec application design principles, guidelines, and concepts together in a comprehensible framework that was envisaged as being useful for the development of secure and usable IS applications. The framework consisted of socio-technical issues that needed to be addressed in developing secure and usable IS applications, thereby providing a usable security property to these applications. The framework was developed from data collected from two sources in mixed methods research. This chapter discusses the research design and methodology of the study by outlining decisions made at every stage of the research process based on the ‘research onion’.

4.2 RESEARCH DESIGN

Research design is the roadmap of the entire research project that outlines choices to be made, from the paradigm (philosophical assumptions) to the intricacies of data collection and analysis; essentially, it is the research plan (Creswell & Poth 2017). Research design deals with issues such as the research paradigm that guides the selection of the research approach, research strategy, and research methods. The choices made at the paradigm level, in turn, provide guidance in the selection of research strategies and data collection and analysis techniques used in finding solutions to the research problem. The definitions assigned to research design and methodology terminology differ from one scholar to the next. In this research, the researcher defined these terms based on the 'research onion' by Saunders et al. (2016). (See Figure 4-2.)

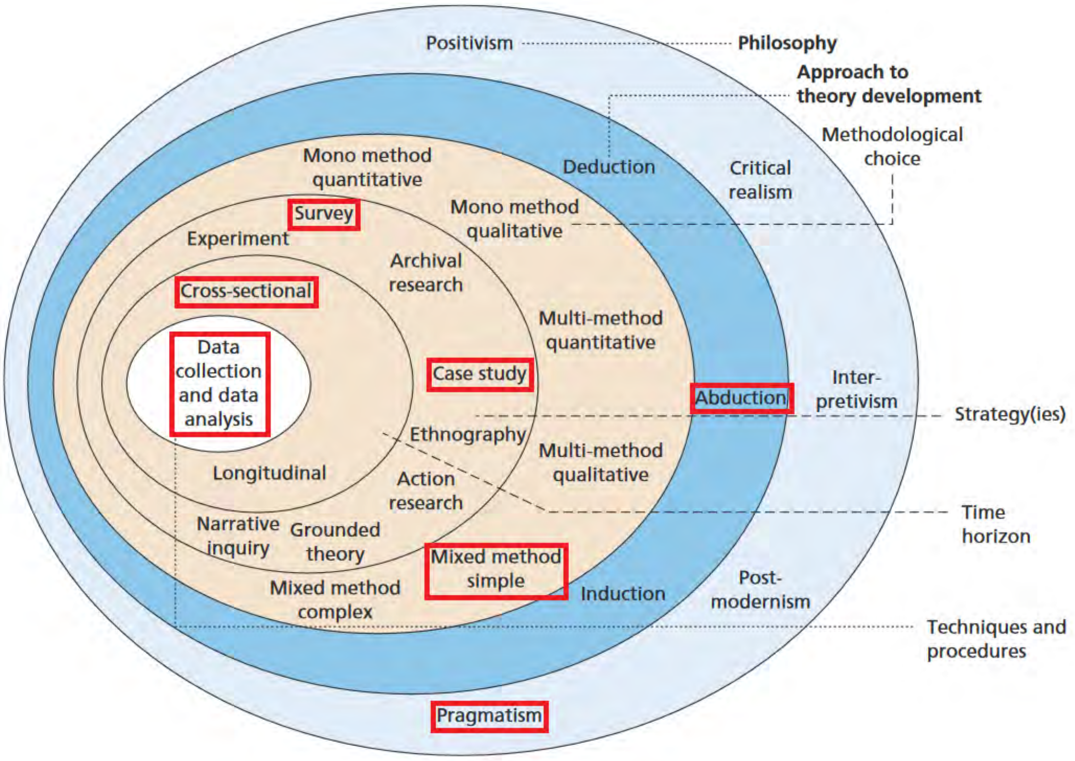


Figure 4-2: The 'research onion'[1] (Saunders et al. 2016)

Figure 4-2 highlights the selected choices at every layer of the research onion with a red rectangle. The chapter gives detailed discussions of the chosen options and motivations for the selections from the outer layer inwards, with limited contextual background on some of the options available at every layer. Research onion layers to be covered in this chapter include philosophy, approach, methodology, strategy, and time zone. The data collection and analysis layer is briefly introduced, with a detailed discussion to follow in chapters 5 and 6. The following sections expand on, and discuss, each choice made at each layer, starting with the research paradigm.

[1] The 'research onion' is reproduced with permission from the author.

4.3 RESEARCH PARADIGM

A research paradigm (also known as a research philosophy or philosophical assumptions) is essentially a basic set of beliefs that guides research, consisting of four aspects, namely, *ethics (axiology)*, *ontology*, *epistemology*, and *methodology* (Denzin & Lincoln 2013). It is the beliefs and assumptions with regard to how knowledge is developed (Saunders et al. 2016). The basic underlying philosophical assumptions concerning what constitutes knowledge and the approaches used to unearth that knowledge are at the heart of a research paradigm (Greene & Hall 2010). *Ethics*, as Denzin and Lincoln (2013) note, deals with moral issues in the course of conducting research. They describe *epistemology* as questions about how one knows the world, while *ontology* is concerned with questions about the nature of reality, specifically what we perceive to be real (Denzin & Lincoln 2013). The authors state that *methodology* refers to the best procedures for acquiring knowledge about the world. A number of paradigms are applicable to information systems and social science research. The research problem or research question(s) will guide the selection of an appropriate paradigm. With regard to the paradigms discussed below, there are also different variations found in the literature. The three paradigms discussed are those with direct links to the chosen paradigm of this research – pragmatism. The paradigms are discussed based on fours aspects: ontology, epistemology, axiology, and methodology.

4.3.1 Positivism

Positivism subscribes to the philosophical stance of the natural sciences, with observable and measurable reality (Saunders et al. 2016). Ontologically, positivism embraces realism; that is, reality exists independent of how social actors label or think about it (Saunders et al. 2016). Positivists believe that reality is objective and can be measured, which leads to an epistemological stance that seeks to discover the objective truth about the real world through measurable metrics that allow universal law-like generalisations (Saunders et al. 2016). This measurement is achieved with properties that are autonomous of the researcher and tools used (Myers 2013). Realism leads positivists to an axiological belief that strives to avoid research values, as these bring bias into their research (Saunders et al. 2016). Because of the objective nature of positivist enquiry, it often uses methodological choices that are typically deductive and highly structured and that include measurement metrics that rely on high samples; it uses predominantly quantitative techniques of data analysis (Saunders et al. 2016).

Positivism is mainly associated with quantitative research that is focused on collecting quantitative data for theory testing to increase the predictive nature of understanding the phenomenon under investigation (Myers 2013). Naturally, positivists adopt an empirical realist ontology that favours empirical evidence, thereby aligning perfectly with scientific-oriented analysis (Fleetwood & Ackroyd 2004). The survey strategy in this research followed the positivism paradigm by objectively investigating the respondents' perceptions of online banking services as provided by South African banks. The survey data was analysed using inferential statistical analysis based on postulated developed hypotheses.

4.3.2 Interpretivism

Interpretivism advocates the need for the researcher to understand humans in their role as social players and sees the difference in doing research among people compared to objects as significant (Saunders et al. 2016). Ontologically, interpretivists believe that the social phenomena we study are constructed by researchers and the researched. Since social actors are unique, it follows that there are multiple realities for each of us (Saunders et al. 2016). Epistemologically, interpretivists believe that research findings are the creation of the process of interaction between the researcher and the researched (Lincoln, Lynham & Guba 2013). Hence, reality can only be accessed through social constructions that include consciousness, language, shared meanings, and tools (Myers 2013). Axiologically, interpretivists are value-bound. Since the researcher is part of the researched, the process is highly subjective, and the researcher's interpretations are key to research contributions. Interpretivism often uses methodological choices that are typically inductive, with in-depth investigations using small samples, typically qualitative methods of data analysis (Saunders et al. 2016).

These meanings can only be obtained by interacting with the participants and looking from the inside, not the outside. As part of the qualitative component of this research, interpretivism was applied through the case study research strategy, which interviewed online banking designers to understand the problem of usable security from the perspective of these participants. This enquiry investigated the challenges financial institutions encountered in the provision of usable security to online digital channels.

4.3.3 Pragmatism

Pragmatism as a paradigm places more emphasis on the research problem and allows the researcher to select the most appropriate approach(es) that can achieve research goals and objectives (Creswell & Creswell 2017). As paradigm, pragmatism is located in the middle of the opposing forces of positivism and interpretivism, giving the researcher the freedom to use aspects of both quantitative and qualitative research methods (Creswell & Clark 2017, Doyle et al. 2009). Pragmatism acknowledges the ontological tenets of both positivism and interpretivism, which are the existence of a single objective reality and that reality is subjective views wedged in the mind, respectively (Creswell & Clark 2017). Epistemologically, pragmatism focuses on practicality; that is, data collection is based on ‘what works’ to address the research problem (Creswell & Clark 2017). The axiological aspects follow multiple stances; for example, both biased and unbiased perspectives are included (Creswell & Clark 2017), and it is value-driven, with the researcher’s doubts and beliefs initiating and sustaining the research (Saunders et al. 2016). Pragmatism is problem-centred; hence, methodological choices are also based on ‘what works’ in addressing the research problem. This leads to pragmatism using a range of methods in the form of mixed or multiple methods from both quantitative and qualitative research (Saunders et al. 2016).

The pragmatic philosophy asserts that human action cannot be separated from experiences and behaviour that has arisen from those experiences; thus, the meaning of actions and beliefs is found in their consequences (Levin & Greenwood 2013). The researcher agrees with this assertion and believes that, in the context of the often-complex InfoSec problem, user behaviour in interaction with IS applications is unique to experiences and understanding of InfoSec problems and awareness. Hence, for solutions that are meant for a wide variety of users, a number of aspects that aid users of different InfoSec awareness levels are critical to providing effective solutions. As such, pragmatic solutions that are not limited by specific philosophical assumptions and methodological choices are necessary to generate new ideas on tackling InfoSec problems.

Morgan (2014) succinctly summarises the relevance of pragmatism by stating that individuals will have different worldviews, as previous experiences are unique, making worldviews both individually unique at the most detailed level and socially shared at broader levels. Hence, pragmatism, unlike other worldviews that emphasise the nature of reality, is more about the nature of experiences. This allows pragmatism to provide a direct connection between theory and praxis (Levin & Greenwood 2013). Johnson and Onwuegbuzie (2004:17) clearly sum up the relationship between pragmatism, on the one hand, and positivism and interpretivism, on the other:

> "*Its logic of inquiry includes the use of induction (or discovery of patterns), deduction (testing of theories and hypotheses), and abduction (uncovering and relying on the best of a set of explanations for understanding one's results).*"

Pragmatism focuses on the research consequences, with primary importance given to (1) the research questions asked rather than the methods and (2) the use of multiple methods of data collection to solve research problems (Creswell & Clark 2017).

4.3.4 Motivation for pragmatism in this study

This research argued that the intersection of human behaviour and security, the subject of this usable security study, is an area that is not straightforward and that conventional solutions have failed to understand the problem and suggest effective solutions. Therefore, applying a pragmatic philosophy that does not view the world through a single lens is likely to contribute significantly to, firstly, understanding the problem and, secondly, proposing solutions. Pragmatism, combined with an MMR design, allows researchers to gain richer and reliable research results in understanding the problem under investigation, as much as research methods are traditionally bound to specific paradigms.

Therefore, to investigate and propose solutions to this complex socio-technical problem of usable security, which has traditionally required a compromise between security and usability goals, the use of pragmatic assumptions was suggested. Pragmatism is seen as providing a different worldview, compared to the extremes catered for in interpretivism and positivism, by focusing on the problem to be researched and the research results (Creswell & Clark 2017, Tashakkori & Teddlie 2010). This paradigm allowed the researcher to answer a research problem that fell in neither the 'traditional' qualitative nor quantitative realms. Pragmatism was also chosen because the research design of choice was MMR, and previous studies have shown that pragmatism is the more appropriate paradigm to accommodate MMR design goals.

4.4 RESEARCH APPROACH

There are mainly three approaches of reasoning to theory development in research: deductive, inductive, and abductive (Saunders et al. 2016). Deductive reasoning typically involves theory and hypothesis testing, evaluated through empirical observations (Gray 2014). Deduction states that if the evidence is true, then the conclusions based on that evidence must also be true (Saunders et al. 2016). This approach is aligned with research that tests a theory by collecting data to make conclusions on an extant theory. Conversely, an inductive approach starts research by collecting data to reach conclusions by generating or building a theory (Saunders et al. 2016). Induction is typically used in qualitative research that uses data collection to explore a phenomenon that is, reasoning from given data to a hypothesis that explains the data (Walton 2014). Abductive reasoning essentially moves back and forth between being deductive and inductive (Saunders et al. 2016); that is, known premises (extant theory) are used to generate testable conclusions to get to the best explanation (Johnson & Gray 2010). Abduction is used to generate or modify theory by incorporating existing theory to build new or modify existing theory (Saunders et al. 2016). Abductive reasoning is mainly associated with pragmatism; deductive reasoning and inductive reasoning are often aligned with positivism and interpretivism, respectively (Venkatesh, Brown & Bala 2013).

In this study, the researcher used the abductive approach that moves back and forth between deductive and inductive reasoning, as this fitted in with the pragmatic MMR design that considers extant theory (UTAUT2) in explaining user behaviour in interaction with InfoSec applications. In this research, quantitative survey data was used to apply the UTAUT2 in the context of online banking as a case study. The objective of using UTAUT2 was to establish the factors that affected service adoption and to later incorporate these findings in the framework. Using interview data, the researcher applied the inductive approach to establish usable security design principles pertinent to online InfoSec applications, as deemed necessary by online banking system custodians. The design principles were drawn from the literature and survey data and then reinforced through interview data open coding. The final set of identified principles from both the deductive and inductive approaches formed part of the final evaluated STInfoSec framework, which was the product of this research.

4.5 METHODOLOGICAL CHOICE

Methodological choice is the third layer in the research onion. Here the choices include three main options, namely, quantitative research, qualitative research, and mixed methods research. These options have further options within each choice. The choice of a design at this layer guides the selection of a research strategy (research method) at the next layer. Quantitative research is often associated with positivism that predominately relies on numerical data (for example, survey data) analysed through quantitative analysis techniques (Saunders et al. 2016). Inversely, qualitative research is suitable for studying a particular phenomenon in depth, especially for exploratory research on a topic that is relatively new, with limited literature (Myers 2013). Quantitative research and qualitative research draw assumptions from opposite ends of the scale of various aspects, some of which have already been discussed in this chapter. In the purest of forms, quantitative research and qualitative research subscribe to objectivism and subjectivism, aligned with positivism and interpretivism, respectively. Quantitative and qualitative research designs consist of variations such as the mono-method and multi-method. The mono-method uses one research method in a study, while the multi-method uses two or more methods that are either quantitative or qualitative, but not both (Saunders et al. 2016). Based on this definition of multi-method research design, an example of such a design is method triangulation, which is discussed below. MMR, however, is a design that uses both quantitative and qualitative research methods in a single study. MMR is discussed in detail later in this section.

4.5.1 Mixed methods research

MMR is a research design that involves philosophical assumptions that allow a mixture of quantitative and qualitative data in a single research study (Creswell & Clark 2017). The emergence of MMR approaches has brought about debate in the general research design discourse. There have been different views, from both 'purist' qualitative and quantitative scholars, on exactly which research paradigm MMR fits into. This has led to the leading qualitative research scholars and advocates (Denzin & Lincoln 2013) discussing the paradigm wars, noting the resistance to mixing methodologies due to different underlying assumptions.

Creswell (2010) and Greene and Hall (2010) note the main argument for resistance to mixing paradigms as the uniqueness of paradigms, while other scholars such as Denzin and Lincoln (2013) contend that paradigms are independent and cannot be combined. Creswell (2010) acknowledges the differences in paradigms – hence, the need to keep them separate in MMR designs. This essentially implies the use of two paradigms in MMR, but the introduction of the pragmatism paradigm provides a paradigm that best suits MMR. In the ongoing discussion of the location of mixed methods in the context of paradigms, Mingers (2001) argues that research methods can be separated from paradigms and can be used critically and knowledgeably to address social problems that are laden with societal and individual self-understandings.

Some scholars advocate the use of pragmatism as the 'more' appropriate paradigm of choice in MMR designs (Creswell & Poth 2017, Morgan 2014, Tashakkori & Teddlie 2010), although others are still sceptical whether it is fit for purpose, as noted in Denzin (2012). Another contentious issue is the exact definition of MMR, which is not surprising, given the different views noted above. Johnson, Onwuegbuzie, and Turner (2007:113) provide a broadly phrased definition of MMR as:

> "[a]*n approach to knowledge (theory and practice) that attempts to consider multiple viewpoints, perspectives, positions, and standpoints (always including the standpoints of qualitative and quantitative research)*".

Regardless of the conflicting arguments, there have been a number of research studies that have aligned MMR with the underlying philosophical assumptions of pragmatism. At the heart of MMR design is the notion noted by Creswell and Clark (2017) that the use of both quantitative and qualitative procedures allows for a deeper understanding of the research problem under investigation compared to the use of one method on its own. The data collection instruments and analysis techniques of these two approaches can either be used in parallel or sequentially, based on the exact MMR design chosen from a number of possible designs. As early as the 1980s, Kaplan and Duchon (1988) began advocating the productive mixture of both qualitative and quantitative research methods to yield richer research findings for a deeper understanding of the research problem. This problem-centred approach of MMR makes the design suitable for adopting pragmatism as a paradigm.

4.5.2 Triangulation

MMR initially began as triangulation, which involves the use of multiple methods in the same quantitative or qualitative approach (Creswell & Clark 2017). This interpretation means that triangulation seeks convergence of findings through validation by using multiple methods to get to the same result (Tashakkori & Teddlie 2010) by showing that the same findings can be reached using different data sets from different methods. At a general level, triangulation is essentially a mixed methods design, although these methods belong to a single research design – quantitative or qualitative (Greene, Caracelli & Graham 1989). As scholars began scrutinising the definition of MMR and the maturity of the design through an increasing number of studies, the definition evolved to specifically imply mixing of quantitative and qualitative research methods in a single study. Triangulation, in the context of positivist research (with the belief that there is a single reality), means that the use of multiple methods leads to a consistent set of results (Oates 2006).

Inversely, in interpretivist research (with multiple realities), the author postulates that triangulation is likely to yield different findings. Denzin (2012) contends that triangulation was originally meant to use multiple forms of qualitative research methods in a single research study, not a mixture of qualitative and quantitative methods. Therefore, the major difference between triangulation and MMR is that MMR collects different sets of data using multiple methods from both quantitative and qualitative approaches and uses the combined results to reach final interpretation. Triangulation uses multiple methods in either qualitative or quantitative research where the findings of one method are reinforced by the findings of the other method. Given the above description of triangulation, it follows that this research did not apply triangulation, since the different data sets in this MMR were not intended for validation of different findings, but to complement each other in answering the research questions.

4.5.3 Motivations for mixed methods research

Morgan (2014) identifies three motivations for using an MMR design: convergent findings, additional coverage, and sequential contributions. He describes these motivations as follows: *convergent findings* use quantitative and qualitative research methods to answer the same research question, mainly to show that both methods arrive at the same conclusion, thereby reinforcing the results with greater certainty. *Sequential contributions* apply research strategies in specific order to enhance the effectiveness of one another in the pursuit of achieving research objectives. *Additional coverage* uses certain strengths of different strategies to achieve different objectives of the same research project. From the above typology, the researcher used *additional coverage* that sought to use different strengths of survey (quantitative) and exploratory case study (qualitative) strategies, with the main objective of identifying appropriate usable design principles to be included in the final framework. The insight of online banking designers, coupled with users' perceptions of the service, achieved the goal of identifying design principles for final evaluation in the framework.

4.5.4 Mixed methods research designs

Numerous authors in the literature advocate different MMR designs. This research considered those methods identified by Creswell and Creswell (2017) to inform the selection. A brief discussion of each of these follows. *Convergent parallel* design is implemented by running two strands separately and integrating the results in the final interpretation. The *embedded* design has either a qualitative or a quantitative design as the main research design, with the other in a secondary role to enrich the overall design. *Explanatory sequential* design uses the quantitative component first, the results of which are used to build up on further examination with a qualitative component, before final interpretation. The *exploratory sequential* design reverses the sequence of explanatory design by applying qualitative research first, followed by quantitative research, before final interpretation. The *transformative* design uses both quantitative and qualitative research in a 'transformative framework' that controls the overall research project (Creswell & Clark 2017). The transformative framework is a mixed methods design that recognises that realities are constructed by various aspects such as social, cultural, economic, political, and ethnic values, and power determines which reality will be privileged (Mertens 2007). Lastly, *multiphase* design consists of more than one MMR study that contributes to a common goal for multiple research projects. According to Creswell and Clark (2017), the convergent design is used to understand the topic, and it primarily follows the philosophy of pragmatism, with both methods having equal emphasis.

Creswell and Clark (2017) specifically identify the convergent parallel MMR design as suitable for pragmatic philosophy, with the other designs aligned with various other paradigms. This research used the convergent parallel MMR design, illustrated in Figure 4-3, with both quantitative research and qualitative research in equal standing, denoted by the

QUAN + *QUAL* notation based on Morse (2010). The quantitative and qualitative research strands collected different types of data that were analysed separately, and these analyses were then combined to feed into the overall final interpretation. The convergent parallel MMR design collects both quantitative and qualitative data because each provides a partial view of the research phenomenon (Creswell & Clark 2017).

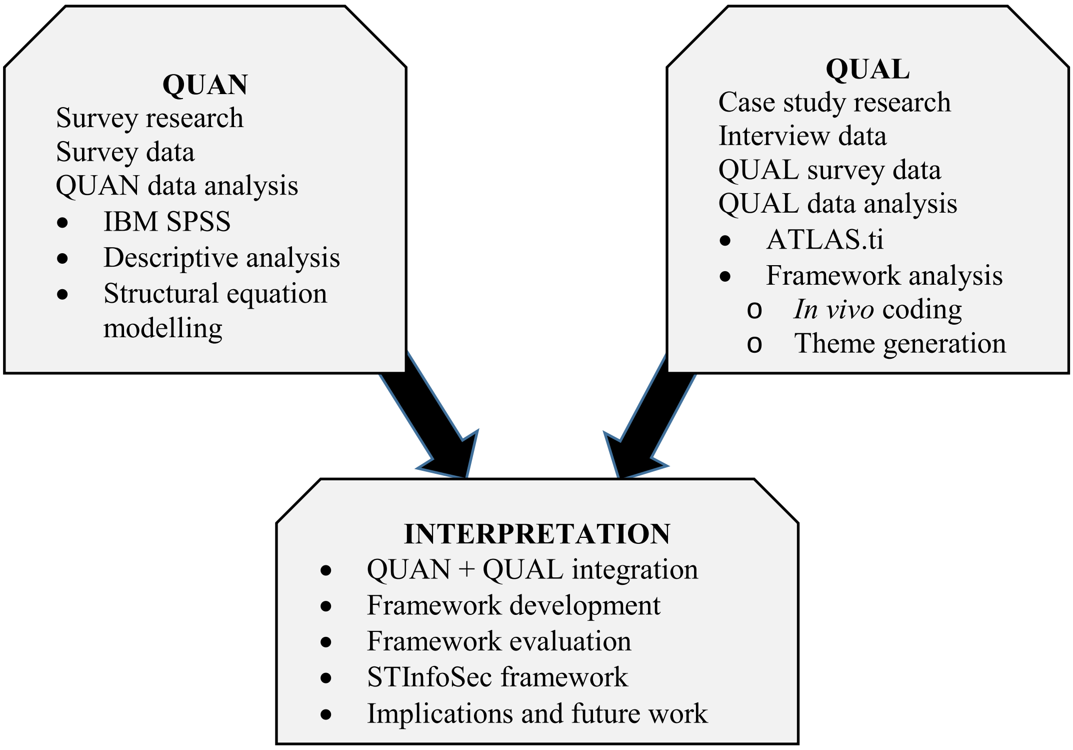


Figure 4-3: Convergent parallel mixed methods design

The design has parallel parts, since each method collects and analyses data independently of the other (Creswell & Clark 2017). The actual data collection can either be sequential or concurrent due to logistical reasons (for example, one researcher collecting both sets of data), but still qualify as a parallel design – since one method does not rely on, or feed its findings into, the other method. In this study, the two sets of data were analysed separately, followed by the final interpretation that combined the findings from the QUAN and QUAL components. Figure 4-3 includes qualitative survey data in the QUAL component. This data was based on the open-ended questions that were part of the survey. The final interpretation fed into the proposed STInfoSec framework for the development of secure and usable online InfoSec applications. Chapter 7 presents the framework in detail.

4.5.5 Motivation for mixed methods in this study

As noted in this section, MMR was used for a number of reasons. The convergent parallel MMR design is mainly suitable when one needs complementarity and completeness, which were this researcher's motivations for applying this design in this research. The rationale of complementarity, as Greene et al. (1989:259) note, is "*to increase the interpretability, meaningfulness, and validity of constructs and inquiry results by both capitalising on inherent method strengths and counteracting inherent biases in methods and other sources*". The completeness of MMR allows the researcher to address the phenomenon under study comprehensively, through collection and analysis of data from both strategies in the same study (Bryman 2006). STInfoSec framework development based on both survey and case study interview data meant that the findings of one method complemented those of the other, thereby providing input from multiple perspectives.

MMR design has advantages, such as bringing the best from both methods. The research methods used in this research allowed users and developers of online applications (using the case study of online banking) to raise aspects pertinent from their perspective, thus giving the researcher a complete picture of the research phenomenon. Through data analysis, the researcher looked to see whether certain issues were raised by both groups of subjects (users and developers), and this provided credibility to the findings. The comprehensive and rich evidence gathered from both sources contributed to the development of a framework for secure and usable online banking user interfaces.

This research, thus, followed an MMR design under the pragmatism paradigm that acknowledged both positivist and interpretivist assumptions to answer the research questions and to achieve the research objectives. The researcher adopted and applied simple interpretation of research choices based on the following MMR design: in the realm of pragmatism, the quantitative strand followed the deductive approach based on a quantitative survey; the qualitative strand adopted a purely inductive approach that collected interview data through an exploratory case study. Although there are numerous ways of using research choices such as paradigms, approaches, and strategies, the researcher adopted the simplistic and conventional meanings of the choices mentioned and motivated earlier, based on the 'research onion'. Hence, the research was aligned strictly with either a quantitative or a qualitative method in the application of each strand.

4.6 RESEARCH STRATEGY

A research strategy is a general plan that helps the researcher to investigate the research problem, answer research questions, and achieve research objectives in a systematic way (Saunders et al. 2016). Effectively, a research strategy is concerned with choosing research methods to be used in a study, with some scholars using the terms 'research strategy' and 'research method' interchangeably. Among the main research strategies to choose from are case study, survey, experiment, ethnography, grounded theory, and action research. Research strategies can be employed for exploratory, explanatory, and descriptive research, and each research method can be used for each of these types of research (Yin 2014).

This research used a combination of two research strategies in an MMR design, namely, a survey and an exploratory case study. Yin (2014) suggests that the use of survey and case study strategies is more suited to research that focuses on contemporary events, that is, events occurring in the present. Online InfoSec is an evolving problem, with many facets, including socio-technical aspects. Essentially, this research took the form of a survey within a case study, where online banking was the case study of online applications and the survey collected responses from online banking users. The combination of survey and case study strategies was used to examine an explanatory causal argument of the many facets of usable security design in the context of online applications. As mentioned earlier, these facets were security and usability, which often exhibited conflicting goals, thus calling for striking a balance in IS design. Next in this chapter, the two strategies chosen for this research are discussed in detail.

The time horizon of this research was cross-sectional, with data collected during a particular time (between June 2015 and September 2016). In contrast, a research study can also be longitudinal and follow a 'diary' perspective, which collects data at more than one point in time (Saunders et al. 2016).

4.7 SURVEY RESEARCH

A survey is a set of questions that respondents, usually individuals, are requested to answer (Lazar, Feng & Hochheiser 2010). This set of questions is generally referred to as a questionnaire; hence, a questionnaire is a data collection instrument used in a survey (Oxford Dictionary 2018). As a research strategy, survey research is a systematic strategy for collecting data from a sample of individuals using a data collection instrument. The survey research strategy is not limited to only a questionnaire as a data collection instrument; other acceptable instruments include observations or interviews.

The survey strategy allows a researcher to gather quantitative data that is analysed quantitatively based on some descriptive and inferential statistical metrics. The analysis allows for suggestions on possible reasons for the existence of relationships between variables and creation of models of these relationships (Saunders et al. 2016). The survey strategy is mostly aligned with the deductive approach and explanatory research. Surveys allow a researcher to investigate more variables contiguously by collecting real-world data from respondents. When measuring a social phenomenon, a major drawback of the survey is the difficulty in unearthing the 'deep' causal effects of the phenomenon under study, as there is no room for asking follow-up questions (Lazar et al. 2010). This drawback can be mitigated by complementing a survey strategy with another data collection instrument such as interviews to ask follow-up questions.

As noted in Chapter 2, compared to other developing economies and the world at large, the online banking adoption rate in South Africa is very low. In this research, the survey strategy was used to investigate the factors contributing to the lack of adoption and to understand the behaviour of online banking users. There are many factors influencing the adoption of online banking and its subsequent continued use after adoption. Hence, it was important to take these factors into consideration when investigating customer attitude and behaviour towards online banking. The questionnaire solicited users' perceptions of the usability of online banking user interfaces. These perceptions allowed the researcher to gain insight into the online banking users' mental models and a better understanding of the users' security behaviour. The questionnaire also asked for the evaluation of online banking service as offered by South African banks.

4.7.1 Sampling

Given (2008) defines a sample as the portion of the target population that is chosen as potential data sources in research. Sampling is the process of selecting possible data sources from a defined larger target population, resulting in a sample size (Given 2008). Sampling decisions followed in a research study have a direct impact on the validity of the findings. Such decisions include the sampling procedure, sample size adequacy, and sample representativeness (Antonius 2013). Data collection that involves samples is usually done with the intention of generalising the findings to the whole population. For generalisation to be valid, the sample must be representative of the population through the use of the appropriate sampling methods and other sampling decisions.

Broadly, there are two types of samples: probabilistic and non-probabilistic. Probabilistic sampling gives each target population unit an equal opportunity for inclusion in the sample. Probabilistic sampling methods include simple random, systematic, cluster, and stratified random. Non-probabilistic sampling does not give each unit of the target population an equal chance of selection. Non-probabilistic sampling methods include a quota, convenience, judgement, and samples of volunteers.

Simple random sampling is the main probabilistic sampling technique that gives each unit in the target population an equal chance of selection. This makes simple random sampling the most reliable sampling method, giving a higher degree of sample representativeness, and this is achieved by inviting each unit in the population to participate in the research. Unfortunately, the simple random sampling method and other probabilistic methods are often impractical, as the population grows, making it difficult and costly to reach and invite each population unit to participate.

This was true in this research; due to the large size of the target population and the difficulty in accessing this population, simple random sampling was impractical and unfeasible. Access to bank clients through banks is always a challenge, even more so when such surveys ask about security and usability of systems. Given the geographical difficulty of accessing all online banking users in South Africa, as banks cannot provide such information due to privacy policies, non-probabilistic sampling was used. As a result of the diverse demographics of the South African population and to ensure a more representative sample, the aim of the survey strategy was to collect demographic information that included the location of respondents, income, home language, and educational qualifications. Based on the analysis of this information, it could be guaranteed, with a certain level of assurance, that the sample was representative of the target population.

Regardless of the drawbacks, non-probability sampling methods are useful in social science research when the population targets are very specific and not readily available (Kitchenham & Pfleeger 2002). Non-probability sampling is also acceptable when the population characteristics are evenly distributed, which makes any sample size large enough to be representative and to generalise the findings to the larger population. This study used mainly non-probabilistic sampling by sending invitations to participate to qualifying respondents through online tools such as email and social media. Efforts to obtain representative samples from all nine South African provinces were made by distributing the survey to potential respondents who resided in all provinces. Based on the characteristics of the online banking users under investigation, the researcher believes that the sampling methods discussed below yielded an accurate and representative sample of the population.

4.7.2 Quota sampling

Quota sampling groups the population based on certain criteria such as gender, income, place of residence, or age (Antonius 2013). In this research, to obtain a representative sample of South African online banking users, the target population was divided into groups based on geographical location (provinces). The respondents were selected using the quota sampling method based on grouping the population by provincial location. In order to generalise the findings to the greater population, the intention was to collect a sizeable number of responses from each province. Table 4-1 provides the contributions of the population of the provinces to the total population and the respective contributions to the GDP of South Africa.

Table 4-1: Mid-year population estimates 2016

Province	Population	Percentage of population	Percentage of GDP
Eastern Cape	7 061 700	12.6	7.7
Free State	2 861 600	5.1	5.1
Gauteng	13 498 200	24.1	33.8
KwaZulu-Natal	11 079 700	19.8	16.0
Limpopo	5 803 900	10.4	7.3
Mpumalanga	4 328 300	7.7	7.6
Northern Cape	1 191 700	2.1	2.0
North West	3 790 600	6.8	6.8
Western Cape	6 293 200	11.3	13.7
Total	**55 908 900**	**100**	**100**

(Stats SA 2016)

It has to be noted that statistics on the location of online banking users were not available, making it difficult to collect proportional responses in all provinces based on the provincial population. Given that Gauteng province accounts for the highest percentage of the population and that it is essentially the economic heart of the nation, the researcher envisaged collecting the majority of responses in this province, allowing for generalisation. The final sample size, therefore, needed to be big enough for valid analysis and to allow for generalisation, since the characteristics of online banking users did not necessarily depend on location.

4.7.3 Sample size

The target population for this research consisted of online banking users from South African banks. Although the exact number of unique online banking users is difficult to calculate, as this number varies based on the source, there are approximately three million online banking users in South Africa across all banks that provide digital banking channels based on figures released by the banks. This number includes a sizeable number of bank account holders who have accounts at multiple banks and have multiple online banking profiles. To make matters worse, banks sometimes also fail to adjust online banking figures to exclude business accounts.

Numerous ways of calculating the sample size can be found in the literature. Based on a 95% confidence level and a 5% margin of error, the required number of responses is 384 for a target population above one million. A sample is a collection of representative research units selected from the target population. The sample size must be big enough and properly constituted to embody all the characteristics of the target population. Regarding sample size for factor analysis in quantitative data analysis, Hair Jr., Black, Babin, and Anderson (2014) recommend a minimum of 100 responses. Chapter 5 provides a detailed analysis of the final sample sizes in this research.

4.7.4 Questionnaire development

The Oxford Dictionary (2018) defines a questionnaire as "[a] *set of printed or written questions with a choice of answers, devised for the purposes of a survey or statistical study*". It is, therefore, an important instrument in collecting deductive data for statistical analysis. Questionnaires are mostly used as a survey strategy for descriptive or explanatory research. The questionnaire in this research consisted of mostly closed-ended questions, with three open-ended questions that asked respondents to provide any additional information they might deem necessary. The questionnaire consisted of six sections, as shown in Table 4-2, together with a detailed breakdown containing the section description and number of questions in each section. The full questionnaire is included as Appendix E.

Table 4-2: Questionnaire description

Section	Description	Items
A: Demographic details	Users' demographic information, e.g. gender & age	8
B: General questions	General banking and online banking questions, e.g. bank name and period of online banking usage	4
C: Acceptance & use	Online banking acceptance and usage constructs	34
D: Usability	Online banking usability evaluation constructs	39
E: Security & privacy	Online banking security and privacy constructs	13
F: Overall assessment	Qualitative overall assessment of online banking	2

The following sections provide detailed information on how the questions were developed based on the theoretical discussions of the constructs provided in Chapter 3.

Section A: Demographic details

The research required the collection of information about respondents to allow for analysis based on a number of moderating factors. Section A collected general personal information about the respondents. The section consisted of eight compulsory questions, asking for the following information that constituted the moderating factors: gender, age, home language, highest educational qualification, employment status, monthly income, location (South African province), and ethnic group.

Section B: General questions

This section asked general banking and online banking questions, which included bank, duration of online banking usage (experience), frequency of online banking login, and device(s) used to connect to online banking. These constituted additional moderating factors for analysis of the results. However, to avoid prejudice and for ethical reasons no analysis was conducted based on the bank names collected in the survey.

Section C: Acceptance and use

Section C consisted of UTAUT2 constructs. The model has been validated by numerous studies to measure the acceptance and continued use of online banking. UTAUT is a unified model of eight individual technology acceptance models. The section consisted of 34 items spread across eight constructs.

Section D: Usability

This research postulates that usability has an effect on adoption, acceptance, and continued use of online InfoSec applications. The questions in this section were based on numerous principles identified in usability studies and, specifically, those related to usable security design principles. The section consisted of 39 items. These included 10 standardised items of the system usability scale (SUS) developed by Brooke (1996) and assessment of six usability constructs with 29 items.

Section E: Security and privacy

Studies on usable security (discussed in Chapter 3) identified a number of design principles to be considered for development of secure and usable applications. This section had 13 items that measured security and privacy constructs.

Sections C through E used an ordinal five-point Likert scale, with values as defined in Table 4-3.

Table 4-3: The Likert scale

Value	Description
1	**Strongly disagree:** the respondent definitely does not agree with the statement.
2	**Disagree:** the respondent possibly does not agree with the statement.
3	**Neutral:** the respondent does not have an opinion about the statement. This can mean that the statement is not applicable.
4	**Agree:** the respondent does agree with the statement.
5	**Strongly agree:** the respondent definitely does agree with the statement.

Lastly, Section F solicited any additional perceptions that respondents might want to add by asking for the overall assessment of the online banking service based on what they liked and disliked most.

4.7.5 Questionnaire distribution

In an effort to reach a representative sample, the questionnaire was distributed both online and physically in different regions of South Africa. Respondents were invited to participate using invitations sent through email and social media that had a link to the Google Forms survey. Questionnaire administration was mainly done online using Google Forms, and the responses were received anonymously, with additional responses obtained through printed questionnaires distributed physically to respondents.

The survey was available online for completion for one year, with regular reminders to encourage participation. Invitations to participate, together with the survey link, were sent to University of South Africa School of Computing and College of Science, Engineering, and Technology staff members. Invitations were also sent to email contacts at the University of Fort Hare, Nelson Mandela Metropolitan University, Central University of Technology, Cape Peninsula University, and University of Limpopo. Requests to participate were sent to information technology mailing groups and online discussion forums, which included AISSAC, SAICSIT, SACLA, MyBroadband, and the SA Forum. Ethical consideration for the research were discussed in section 1.6 of Chapter 1.

4.7.6 Research model and hypotheses

Section C of the survey covered UTAUT2 constructs and moderators. The research model was an adaptation of the latest UTAUT2 by Venkatesh et al. (2012), which explains the general adoption and use of information systems based on various constructs and their relationships. UTAUT2 is an improvement of the original UTAUT by Venkatesh et al. (2003), with three additional constructs, namely, hedonic motivation, price value, and habit, while voluntariness of use was dropped as a moderator. The proposed research model retained UTAUT2 constructs and provided additional moderators that were specific to InfoSec systems in a South African online banking context. Literature review in the area of user acceptance and continued use of information technology yielded a number of constructs that were measured by checklist items. After a thorough analysis of this literature, the research selected the constructs to be examined. The details of the research model, research hypotheses, and constructs under investigation are outlined in Chapter 5. The instrument intended to gather and analyse online banking users' perceptions of the current online banking service. The research model included constructs that were identified to be pertinent to investigate the usability of online banking interfaces in the South African context, a context that included users with a diverse cultural and language background.

4.7.7 Instrument validity and reliability

Validity of a survey instrument simply means that the instrument measures what it is supposed to measure, while reliability is the ability of an instrument to measure the same phenomenon consistently, assuming that what is being measured remains constant (Antonius 2013). It addresses both the content and detail of the research issues under investigation. This can be achieved by conducting an extensive literature review during the development of the instrument items and using standardised survey items from previous research studies. The scale of reliability ranges from 0.00 to 1.00, denoting very unreliable and perfectly reliable, respectively (Gray 2014). Cronbach's alpha is an objective measure of instrument reliability that IBM's Statistical Package for the Social Sciences (SPSS) is capable of computing. Reliability and validity are closely related, as an instrument can only be reliable if it is valid, but its validity does not depend on its reliability.

4.7.8 Quantitative data analysis

The quantitative survey data was analysed using IBM SPSS and Amos software packages. These packages are capable of performing a number of descriptive and other advanced statistical analyses, including factor analysis and regression and correlation analyses of model variables. These techniques allow for the investigation of relationships among independent and dependent variables in a research model. Amos comes as an additional module to SPSS and provides graphics features to draw network diagrams depicting relationships among variables as analysed by various structural equation modelling techniques. Chapter 5 provides details of quantitative data analysis techniques applied in this study.

4.8 CASE STUDY RESEARCH

A case study is appropriate in explaining some present circumstance and understanding some social phenomenon. Lazar et al. (2010) define 'case study' as "*an in-depth study of a specific instance (or small number of instances) within a specific real-life context*". It helps in understanding complex social phenomena (Yin 2014). According to Creswell and Poth (2017), there are mainly three kinds of case studies: an intrinsic case study, an instrumental case study, and a collective case study. An intrinsic case study is a case study chosen for its uniqueness, irrespective of its applicability in other situations, while an instrumental case study is one that studies a phenomenon that can be applied to other similar situations (Creswell & Poth 2017). A collective case study studies one issue of concern in multiple cases (Creswell & Poth 2017). The case study in this research could be classified as an instrumental case study because the resulting framework was envisaged to be applied, with minimum adaptation, to similar situations to develop secure and usable online InfoSec applications.

Research case studies can be applied for discovery in exploratory research or for testing, for explanation, or for comparison in explanatory research (Myers 2013). The above implies that case studies can be applied in traditionally quantitative studies that attempt to test theory and traditional qualitative studies that generate theory. This research used exploratory case study research to complement the overall findings of the research study. The case study assisted in investigating the perceptions of online banking custodians with regard to taking user behaviour into account in the development of online InfoSec applications.

Online banking was chosen as the case study for online information system security applications. The researcher envisaged that the proposed framework would be applicable to other online information system security applications that had the same characteristics as online banking. These characteristics included the need for security and privacy and user interfaces that were both usable and catered for UX, while providing core functionalities. These characteristics foster adoption and continued use of such applications. Given the arrival of numerous online applications that convey confidential and sensitive personal information for both individuals and organisations through the internet, designs that cater for security and privacy are vital. At the same time, these applications need to provide users with additional non-functional aspects of the systems such as satisfaction and user experiences that make users want to continue using them. An investigation that includes obtaining users' perceptions of the current state of affairs, as well as the challenges developers of these systems face, can help provide a complete picture of the problem.

This research, therefore, investigated human behaviour in interaction with InfoSec applications, specifically the effect of usability and UX attributes during design, to enable users with diverse backgrounds to effectively and efficiently use InfoSec applications. To understand this phenomenon, the researcher selected online banking service as a single instrumental case study, and the findings could be applicable to other InfoSec applications with the same characteristics.

There are numerous sources of data in case study research, which include observation, interviews, digital media, and documentary analysis. This research collected data using interviews with online banking service personnel as participants selected from South African financial institutions. The target participants were practitioners in InfoSec application design, including usability and UX practitioners in InfoSec applications development. These participants were selected because they had knowledge of decisions made in the process of developing these applications, and such knowledge would assist in achieving the main objective of this research.

4.8.1 Interviews

Interviews in research are one of the main sources of data for qualitative research methods. An interview mainly involves the human interaction between an interviewee (usually the research participant) and the interviewer (usually the researcher). The interviewer asks the interviewee predetermined questions. Unlike in a self-administered survey, in an interview, the researcher can ask follow-up questions to obtain more insight into a particular issue. Interviews can either be quantitative (structured) or qualitative, where qualitative interviewing includes unstructured, semi-structured, and in-depth interviewing (Yin 2016).

Structured interviews are similar to the questionnaires often applied in quantitative data collection, where all participants are asked a set of predetermined and standardised questions by the interviewer (Gray 2014). Structured interviews usually use closed-ended questions that have predefined responses, and they are mainly used to ask interviewees the same set of questions in the same order (Yin 2016).

Semi-structured interviews do not use a standardised set of questions; instead, the interviewer prepares an interview schedule, with a list of questions and themes to be addressed in an interview (Gray 2014). In semi-structured interviews, the interviewer may decide not to ask all the questions during an interview and may also ask additional probing questions that are not on the interview schedule. This allows the researcher to probe for additional information that was not originally planned for before the interview session, giving additional insights into the research problem. Interview questions are asked in any order from one interview to the next based on the flow of the conversation. This requires audio recording for transcription into text before analysis in order to capture all the interview data.

Unstructured interviews have no predetermined interview questions, and usually, no time limit is set, allowing the interviewee to freely say anything he or she wants (Myers 2013). During breaks in conversation, the interviewer improvises to come up with the next question to ask the interviewee. The lack of a predetermined list of questions means that the interviewer needs a deep and clear understanding of the aspects explored in an interview session (Saunders et al. 2016).

This research used semi-structured interviews to solicit views from InfoSec design experts in online banking applications. The specific target participants were InfoSec technicians for online banking applications, InfoSec mid-level management from financial institutions, and general usability and UX practitioners. The interviews sought to gather information about the standards and best practices employed by financial institutions in addressing usability and UX issues in information systems. Interviews enable qualitative researchers to get closer to research subjects and get deeper insight from the participants' perspective into the research problem under investigation (Denzin & Lincoln 2013).

4.8.2 Purposive sampling

Purposive sampling allows the researcher to choose a sample based on some features of the study, mostly useful in selecting participants in interviews or focus groups (Silverman 2014). It is virtually synonymous with qualitative research, and numerous sampling strategies are classified as purposive sampling, including stakeholder sampling, typical case sampling, and criterion sampling, to mention but a few (Given 2008). Stakeholder sampling involves identifying specific stakeholders in a study that, for instance, evaluates a specific policy development programme. Typical case sampling sets out to identify a case study because it is not unusual to study the simplest case for the phenomenon under investigation (Given 2008).

This research used criterion sampling to select interview participants in this case study, which allowed the researcher to choose participants who fit a specific criterion that contributed to attaining the research objectives (Given 2008). Interview participants were selected based on their InfoSec employment in financial institutions, especially those involved in the design and development of online banking systems. The sample came from the major banks in South Africa. These participants were chosen because they had knowledge of how online banking systems were developed and could give insight into the decision-making process involved with regard to InfoSec, usability, and UX.

4.8.3 Development of interview questions

The interview questions used for qualitative data collection are provided as Appendix F. The questions were developed based on the literature on information system development and usable security design best practices. The questions solicited the current practices based on local and international standards and local legislation governing the financial industry. Also included in the questions were aspects of legacy information technology (IT) systems, InfoSec, usability, UX design considerations, and user awareness and training initiatives as they apply to online information system development.

4.8.4 Qualitative data analysis

Qualitative data is analysed using, for example, the ATLAS.ti software package that performs content analysis to uncover categories by counting the number of occurrences of these in text such as transcribed interview data. ATLAS.ti generates unique codes from text, which the researcher can categorise into themes for interpretation. Chapter 6 gives details of the qualitative data analysis techniques applied in this study – framework analysis.

4.9 CHAPTER CONCLUSION

This research involved collecting both quantitative and qualitative data to obtain the views and perceptions of users and developers of online banking. As such, the chosen paradigm was pragmatic to accommodate both quantitative and qualitative philosophical assumptions. Using the research onion, the chapter outlined choices made in each stage of the research process. Given the MMR design in this study, the researcher chose the abductive reasoning research approach, which moved back and forth between deductive and inductive reasoning. The two research strategies in this research fell in both the quantitative (survey) and qualitative (case study) research methodologies, thereby advancing the application of the research paradigm of pragmatism. Using a convergent parallel mixed methods design, the two strands collected and analysed the data separately for an integrated interpretation. Structural equation modelling and framework analysis were the data analysis techniques used on the quantitative and qualitative data, respectively. These are covered individually in Chapters 5 and 6.

-- oOo --

CHAPTER 5 QUANTITATIVE DATA ANALYSIS

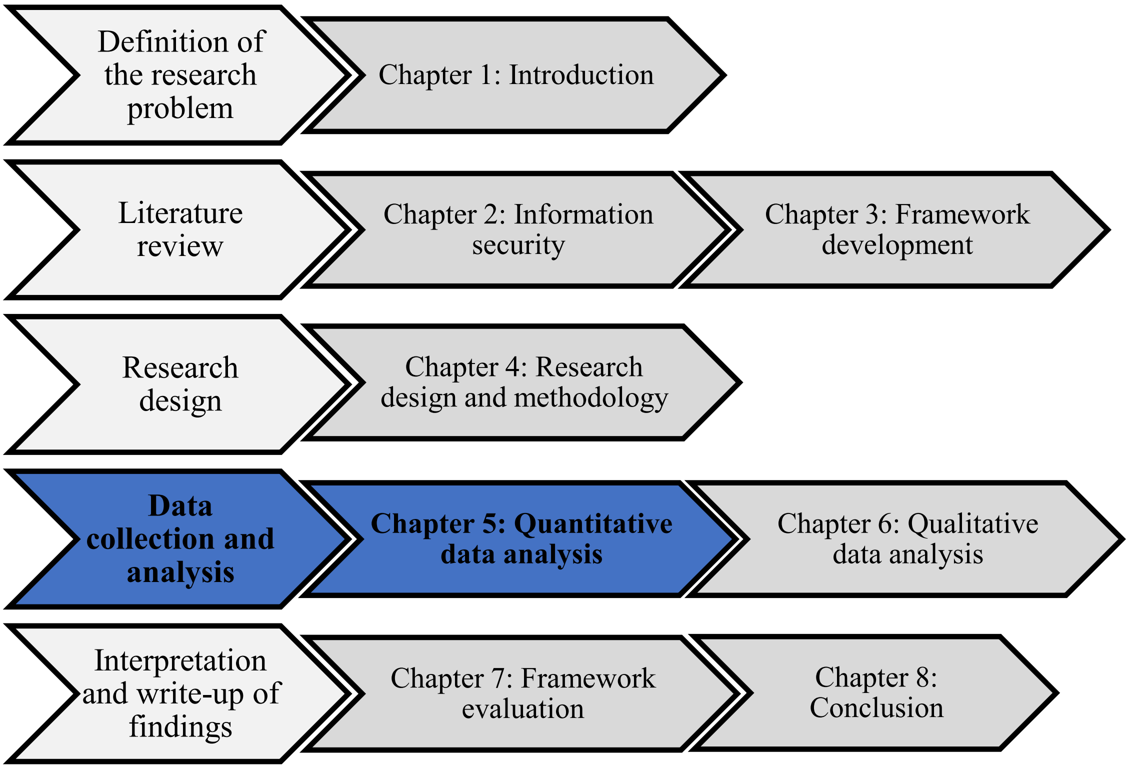

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 5-1: The research roadmap

5.1 INTRODUCTION

Chapter 4 outlined the blueprint for how the research was conducted, including data sources and collection techniques in an MMR design. This chapter is the first of the two data collection and analysis chapters. The purpose of this chapter is to present the quantitative part of the MMR design, highlighting all decisions pertaining to data collection and analysis from the tools and techniques used. The chapter first provides the theoretical framework that guided the data collection and outlines the postulated research hypotheses to be tested. The data collection section begins with determining the type of data required, followed by the selection of the data collection tools and determination of the sample from the population. This is followed by a discussion of research validity and reliability, including reliability analysis of the quantitative data collection instrument. Descriptive analysis is furnished that provides an overview of the respondents, followed by inferential analysis that presents a structural model of the theoretical framework of the research. Lastly, the chapter outlines the final interpretation of the results and discusses the findings in relation to the research questions stated in Chapter 1.

5.2 DATA COLLECTION

Quantitative data was collected using survey research, with a questionnaire as the data collection instrument. (See Appendix E.) The instrument was distributed through the Google Forms online survey tool. The landing page of the survey tool contained a short description of the research and the consent form, where respondents were required to tick a mandatory checkbox to accept and agree to participate in the research. For ethical reasons, respondents were informed of the anonymous nature of their participation in the research and their right to withdraw from participation at any time before submitting responses.

The questionnaire consisted of the following sections: demographic details of respondents, general online banking questions, online banking acceptance and use construct statements, usability constructs (including a 10-item system usability scale), security and privacy statements, and qualitative overall assessment questions. Current online banking users with any of the South African banks were eligible survey respondents. The raw data exported to a Google spreadsheet was transferred to an IBM SPSS Statistics 24 data file for data cleaning and preparation for statistical analysis. (See Appendix G for a sample of responses.)

There were 540 valid and usable responses. This chapter provides details of the statistical analysis techniques implemented and their respective findings. In terms of sample size, there are significantly different opinions on the appropriate sample size in factor analysis and other advanced statistical analyses, which give rise to varying guidelines and rules of thumb on sample size. Tabachnick and Fidell's (2014) rule of thumb suggests at least 300 responses, while Hair Jr. et al. (2014) recommend at least 100 responses. A more detailed guideline is given by Comrey and Lee (1992): 100 (poor), 200 (fair), 300 (good), 500 (very good), and 1 000 or more (excellent). This research reports on a sample of 540 responses, which is regarded as a very good sample size based on these guidelines.

5.3 DATA ANALYSIS

The theoretical model considered three aspects of online banking, namely, adoption and continued use, usability, and security. Online banking adoption was evaluated using the unified model of IT adoption, UTAUT2. Usability was measured using two methods: first the system usability scale with 10 standardised survey items and then six usability constructs consisting of 29 survey items. Security and privacy were evaluated using 13 survey items divided into two constructs. Data analysis was conducted using the IBM SPSS, also known just as SPSS, which is a software package that provides tools for statistical analysis of quantitative data. IBM SPSS Statistics 24 was used, in conjunction with the IBM SPSS Amos 24 software package, which allows for modelling of network diagrams depicting relationships among variables.

5.3.1 Validity

The validity of a survey instrument is about accuracy (Nardi 2014), which simply means that the instrument measures what it is supposed to measure (Antonius 2013). Validity mainly depends on what is being measured, since a tool might not be valid for a certain measure, but perfectly valid in another study. Validity can be achieved by using a tool that has been accepted as a standard in assessing a phenomenon. There are three main types of validity: content validity, construct validity, and criterion (concurrent) validity. Content validity is usually consensus developed among researchers on whether a tool measures what it is supposed to measure (Nardi 2014). Construct validity is the accuracy of a set of items or questions measuring a construct, usually only achieved during data analysis (Nardi 2014). Criterion validity compares findings of construct measurement with similar external criteria or standards (Nardi 2014). Statistically, criterion validity can be measured using Pearson’s *r* in IBM SPSS.

5.3.2 Reliability

Reliability is concerned with two aspects, namely, consistency and replicability (Antonius 2013). Consistency is the ability of an instrument to measure the same phenomenon consistently, assuming that what is being measured remains constant (Nardi 2014). Replicability means that if another measurement is made by a different researcher in different, but similar, circumstances, roughly the same results will be obtained (Antonius 2013), that is to say, the instrument addresses both the content and detail of the research issues under investigation. This can be achieved by conducting an extensive literature review during the development of the research instrument items and using standardised survey items from previous research studies.

Reliability and validity are closely related, as an instrument can only be reliable if it is valid, but its reliability does not depend on its validity. As Hair Jr. et al. (2014:94) put it, "[r]*eliability is a necessary but not sufficient condition for validity*". The scale of reliability ranges from 0.00 to 1.00, denoting totally unreliable and perfectly reliable, respectively (Gray 2014). The reliability of instrument items measures the degree to which a set of items that predict a construct is internally consistent based on how highly interrelated the items are to one another (Hair Jr. et al. 2014).

The survey instrument was tested for reliability to ensure that the instrument measured correct, relevant, and related data before conducting more advanced statistical analyses. In this research, Cronbach's alpha (α), also known as the alpha coefficient, was used to test the reliability of the overall instrument as well as that of all the constructs. Cronbach's alpha was extracted from SPSS, and the results showed that the reliability of the whole measuring instrument was 0.895, as indicated in Table 5-1. Thus, the questionnaire was deemed reliable and could be used.

Table 5-1: Research instrument reliability statistics

Cronbach's alpha	Cronbach's alpha based on standardised items	Items
0.895	0.920	102

Cronbach's alpha obtained for the whole instrument showed that the instrument used in this research was reliable, as it was above the threshold value of 0.70 suggested by other researchers (Pallant 2013). The research, furthermore, investigated the reliability of each construct independently. Table 5-2 shows the results of Cronbach's alpha of each construct as extracted from SPSS, ranging from 0.196 to 0.929. The theory suggests the deletion of construct items that cause the reliability of the construct to be low and below the threshold value of 0.70 (Pallant 2013); the constructs with values below 0.70 are highlighted in Table 5-2. However, in this research, the decision was made not to delete, but to carry over, each construct for further analysis. It is important to note that this decision was based on the fact that, when measuring model fitness in structural equation modelling (SEM) using Amos, one or more construct items and latent variables are highly likely to be deleted. This is in order to achieve model fitness; hence, in such scenarios, deletion priority would be given to construct items, followed by latent variables, as suggested during reliability testing, in that order. However, based on model fitness tests conducted later (See section 5.6.1), the need to delete any construct was avoided as the individual measurement models passed goodness of fit.

Table 5-2: Construct reliability statistics

Construct	Cronbach's alpha	Cronbach's alpha based on standardised items	Items
UTAUT2			
Performance expectancy (PE)	0.764	0.811	5
Effort expectancy (EE)	0.870	0.872	6
Social influence (SI)	0.876	0.881	4
Facilitating conditions (FC)	0.578	0.679	4
Hedonic motivation (HM)	0.880	0.882	4
Price value (PV)	0.929	0.930	3
Habit (H)	0.715	0.735	5
Behavioural intention (BI)	0.704	0.711	3
Usability			
System usability scale (SUS)	0.555	0.536	10
Learnability (UL)	0.877	0.886	5
User suitability (UUS)	0.518	0.600	3
Satisfaction (US)	0.843	0.855	5
Availability (UA)	0.196	0.196	5
Errors (UE)	0.632	0.636	5
Help and documentation (UHD)	0.676	0.676	6
Security and privacy			
Security (S)	0.734	0.737	6
Privacy (P)	0.911	0.913	7

Based on the results of reliability in Table 5-2, the latent variables to be considered first for deletion were availability (usability), user suitability (usability), system usability scale, facilitating conditions, behavioural intention, errors (usability), and help and documentation (usability), respectively.

Table 5-2 shows that the Cronbach's alpha values for UTAUT2 constructs were mostly above the threshold except for FC and BI. This is so because UTAUT2 is a validated model with constructs that have been refined over a period of time through numerous studies. Inversely, the subjective nature of usability makes the construct reliability fluctuate based on the exact system being evaluated by generic constructs. As such, the constructs are not validated across different systems. Therefore, the current study evaluated online banking using generic construct items that were not intended for online banking specifically, resulting in reliability scores below the threshold. This study was the first to develop construct items for online banking, and these can be refined in subsequent studies towards a validated set of constructs for online banking evaluation.

5.4 DESCRIPTIVE STATISTICS

Descriptive statistics allow a large quantity of data to be summarised in limited numerical values, highlighting the most important data features, for example, the percentage of male versus female respondents. Frequency tables are the basic form of descriptive statistics. The metrics in descriptive statistics include mean, median, standard deviation, percentiles, variance, and correlation coefficient. This section outlines the most basic frequency statistics from the sample of the population as extracted from valid survey responses.

The research considered those demographic factors that were predicted to have an explanatory value for the research and to show differences in behaviour and perceptions among groups. Demographic variables served the purpose of providing a means to explain the difference in adoption or use of information and communications technology (ICT) among different groups. Other researchers such as Venkatesh et al. (2012) view demographic factors as having a moderating effect on certain hypothesised relations – therefore, terming them moderating factors.

The UTAUT2 model that informed this research investigated age, gender, and experience as leading factors moderating various relationships in the model. Based on the literature and in the context of online banking, additional moderating factors were considered. These moderating variables included education, employment, ethnicity, and device. Moderating factors allow for an enhanced analysis that separates respondents into different groups and reports on significant differences in behaviour. Table 5-3 shows an extract of the frequencies (the complete table with all factors measured is presented as Appendix H) from the survey based on the demographic factors and general online banking sections of the total sample size of 540.

Table 5-3: Sample frequencies (*n*=540)

Factor	Category	Frequency	Percentage	Cumulative percentage
Gender	Male	314	58.1	58.1
	Female	226	41.9	100.0
Age	Below 20 years	26	4.8	4.8
	20-29 years	122	22.6	27.4
	30-39 years	195	36.1	63.5
	40-49 years	88	16.3	79.8
	Above 50 years	109	20.2	100.0
Education	No formal education	3	0.6	0.6
	Matric	58	10.7	11.3
	Post-matric certificate/diploma	124	23.0	34.3
	Degree	104	19.3	53.5
	Postgraduate degree	239	44.3	97.8
	Other	12	2.2	100.0
Experience	Below 1 year	39	7.2	7.2
	1-2 years	46	8.5	15.7
	3-4 years	96	17.8	33.5
	5-6 years	97	18.0	51.5
	7 years and above	262	48.5	100.0
Use frequency	Every day	185	34.3	34.3
	Once a week	214	39.6	73.9
	Once in two weeks	71	13.2	87.1
	Once a month	65	12.0	99.1
	Other	5	0.9	100.0

More than half of the 540 respondents (58.1%) were males, while 41.9% were females. The largest proportion (36.1%) of respondents came from the 30-to-39-year-old age group, followed by those aged between 20 and 29 years (with 22.6%). Thus, in this research, 75.4% of respondents were aged below 40 years, with 20.2% aged 50 years and above.

In terms of education, 63.5% of respondents had a degree or higher qualification, with a significant portion of 44.3% holding a postgraduate degree. Only three respondents indicated that they had no formal qualification, while 12 respondents selected ‘other’ under qualification.

The results, furthermore, showed that the majority of respondents (66.5%) had five years or more experience of using online banking, while 48.5% had more than seven years’ experience. McLellan, Muddimer, and Peres (2012) found that users with more extensive experience of a product tended to provide more favourable system usability scale scores than novice users. This finding was regardless of the domain product type. Hertzum, Molich, and Jacobsen (2014) investigated the evaluator effect on system usability using 19 experienced participants. Their findings showed that evaluators picked up different sets of positive and negative usability aspects of the system. The implication of this result was that experience acquired in the use of online banking would play an influential role in the perceptions of users towards the technology and that such respondents would provide valuable perceptions compared to those of novice users.

Use frequency results showed that a good number of participants (39.6%) used online banking once a week, followed by 34.3% of respondents who used it daily. In total, close to three-quarters (73.9%) of respondents used online banking at least once a week. Few participants in this research (12.0%) used online banking once a month. These were likely to include formally employed individuals who used online banking to do major transactions that occurred probably once a month after payday, such as monthly household bill payments. Further analysis of use frequency revealed that the majority of 185 daily users (83.8%) mainly used a mobile device to access online banking, while almost half (49.7%) used all three devices and only 23.2% used a single device.

The following frequencies are excluded from Table 5-3 but provided as part of Appendix H. The results showed that English was well represented, with 44.6% of the participants having English as their home language, followed by Afrikaans with 21.6%. It is important to note that 6.9% of the respondents did not indicate their home language; these could be foreign language speakers who opted not mention their home language.

Respondents were asked to indicate their employment status based on five categories. The overwhelming majority were formally employed at 79.8%, followed by 9.8% who were self-employed. Regrouping of employment status created two distinct groups – employed (89.6%) or unemployed (10.4%), with unemployed consisting of retired and other.

The research also investigated the income of the respondents. The results indicated that most respondents (23.7%) earned between R30 000 and R39 999 per month, followed by 22.8% of the respondents who earned more than R50 000. When treated as a binomial variable with the lower-income group earning less than R30 000 and the high earners earning R30 000 and more, the results showed that the majority (55%) were high earners.

Respondents were asked to indicate the province of their current location, and the research indicated that all South African provinces were represented. Gauteng had the highest representation with 46.3% of the respondents, followed by the Western Cape and KwaZulu-Natal, which had 25.7% and 10.9%, respectively. North West and Mpumalanga had the fewest respondents with only 0.9% and 0.6%, respectively. White ethnicity was the largest group with 43.3%, followed by black with 36.7% of respondents, while 15.7% and 4.3% belonged to the Indian/Asian and coloured ethnic groupings, respectively.

The survey asked respondents to identify the bank on which they based their responses. A total of 97.8% of respondents were clients from South Africa's five major banks. Due to ethical concerns, no analysis beyond frequencies is reported on bank names. Generally, the number of respondents for all banks was widely spaced, which showed that the research tried to balance the number of respondents for each bank. Therefore, the moderation results obtained by this research were likely to be representative of the population of South African banks represented in this sample.

The research also asked respondents to list the devices they frequently used to access online banking. The results showed that mobile devices were the most frequently used device (73.7%) to access online banking, followed closely by personal computers with 72.2%, while laptops/portable computers had a percentage of 61.3%. Furthermore, 70% of respondents used more than one device to access online banking, with 37.4% using all three devices, and 30% used a single device. Regrouping device combinations according to respondents who used one device as opposed to those who used more than one device, the results showed that 75.2% of respondents used more than one device to access online banking, while only 24.8% used only one device for all their online banking activities.

5.5 INFERENTIAL STATISTICS

Inferential statistics consists of two main techniques, namely, estimation and hypothesis testing, which are used to draw conclusions about the population based on sample data. This section outlines the estimation parameters applied in this research to generalise the findings to the general population of online banking users in South Africa.

Firstly, estimation is concerned with the margin of error, which acknowledges the lack of precision in the measurements and conclusions of this research, as a sample is likely to differ from the population (Hair Jr. et al. 2014). Specifically, probability of error measures the risk that research estimates are wrong; this is complementary to the level of confidence, as added together they are equal to 100%. All analyses and estimates in this research were based on a 5% probability of error and 95% level of confidence.

Secondly, hypothesis testing provides a means to make propositions about the population based on sample findings and to test for acceptance or rejection of such statements. Hypothesis testing is described in the structural equation modelling (SEM) section of this chapter – all based on the above-mentioned estimation parameters. Before going into SEM analysis, the building blocks of SEM, which include principal component analysis and factor analysis, are outlined.

Quantitative data analysis often involves the investigation of the relationships among multiple variables to postulate a research phenomenon. This gives rise to the need for multivariate analysis, which refers to any statistical technique that analyses data involving more than one variable (Rencher & Christensen 2012). Multivariate data analysis is made easy through an array of statistical packages that utilise the inexpensive computing power of today. Factor analysis is one such multivariate data analysis technique. Hair Jr. et al. (2014) define factor analysis as "*an interdependence technique whose primary purpose is to define the underlying structure among the variables in the analysis*". Factor analysis essentially provides tools for analysing the structure of the correlations among many variables by identifying sets of variables (also known as factors) that are significantly interrelated (Hair Jr. et al. 2014). Strictly speaking, there are two types of factor analysis, namely, exploratory factor analysis and confirmatory factor analysis, both of which use principal component analysis as factor extraction technique.

Principal component analysis (PCA) is a method for extracting constructs from a given set of variables (survey items) based on the correlation among items (Williams, Onsman & Brown 2010). In essence, a principal component is a linear combination of observed variables that are optimally weighted (O'Rourke & Hatcher 2013). PCA differs from factor analysis in that, while principal components are linear combinations of the observed variables, factor analysis factors are the observed variables viewed as linear combinations of the underlying factors (O'Rourke & Hatcher 2013). In factor analysis, PCA is essentially used for factor extraction. The difference between PCA and factor analysis is that factor analysis assumes the existence of an underlying causal model, while PCA is simply a variable reduction technique (Hair Jr., Hult, Ringle & Sarstedt 2016). Exploratory factor analysis (EFA) is a part of factor analysis that extracts the underlying factor structure from a large set of data (O'Rourke & Hatcher 2013). Factors in EFA are derived from analysis of data, not before analysis or from existing theory (Brown 2015). EFA is a technique in factor analysis whose overarching goal is to identify the underlying relationships among measured variables. The most common type of factor analysis is R factor analysis, which analyses a set of variables to identify the dimensions that are latent (or concealed) (Hair Jr. et al. 2014). This research was based on an existing theoretical framework with known variables; hence, confirmatory factor analysis was the most appropriate technique.

In confirmatory factor analysis (CFA), the researcher specifies both the number of factors and the set of variables for each factor loading before computing the analysis (Brown 2015). CFA is, therefore, appropriate to testing a proposed model as part of structural equation modelling. As such, CFA has hypotheses based on extant theory with regard to the factors that describe the proposed model and needs to be based on a strong conceptual model (Brown 2015). Essentially, CFA is a component in SEM that provides the measurement part of SEM, which shows relationships among latent variables and their indicators. SEM, furthermore, provides the structural (path analysis) component part, which shows how the latent variables of interest are related (Hair Jr. et al. 2016).

5.6 STRUCTURAL EQUATION MODELLING

SEM is a popular multivariate analysis technique, as it can simultaneously estimate multiple dependence relationships and incorporate multiple measures for each concept (Hair Jr. et al. 2014). The ability to *simultaneously* estimate multiple dependence relationships makes SEM more powerful than other tools such as multiple regression, factor analysis, and discriminant analysis. SEM is an extension of several other multivariate techniques, including multiple regression analysis and factor analysis (Hair Jr. et al. 2014), which are building blocks to the more advanced SEM analysis. Hence, before going into the details of the SEM technique, brief descriptions of the other analysis techniques that are building blocks of SEM are given.

SEM depicts relationships among constructs, which are dependent and independent variables, involved in the analysis. SEM consists of two models: the measurement model that shows how measured variables represent constructs and the structural model that shows how constructs are related to one another (Hair Jr. et al. 2014). The measurement model is also referred to as confirmatory factor analysis. Constructs are unobservable or latent factors that are represented by multiple variables (Hair Jr. et al. 2016). SEM depicts the relationships in a model, which is essentially a representation of a theory. The SEM model depicts constructs as ovals or circles and measured variables as squares or rectangles. A dependence relationship is shown by means of a solid straight arrow from an independent variable to a dependent variable, while a correlational relationship is depicted through a curved double arrow. Selim (2005) posits that the measurement model is assessed for fitness and fixed first before the structural equation model is examined.

SEM is a model that specifies interdependent relationships between the independent and dependent variables. The hypothesised relationships between latent variables, also called constructs, are called structural models. Ho (2006) advocates that SEM has the advantage of taking into consideration the strength of multiple regression analysis, factor analysis, and multivariate ANOVA in a single model that can be evaluated statistically. In the same regard, SEM has the advantage of testing both the hypothesised paths and possible relationships among the model constructs (Selim 2003). Furthermore, SEM has the ability to test for mediating relationships between predictors and an outcome (Blanthorne, Jones-Fraser & Almer 2006).

SEM has many uses. In this research, SEM was used for theory testing based on theorised concepts on online banking acceptance and multigroup analysis based on moderating factors. Other SEM uses that did not form part of this investigation include mediation/tests of indirect effects, longitudinal models, and multilevel nested modelling. A number of goodness-of-fit measurement models generated from Amos were extracted and reported on. Where maximum goodness of fit was not achieved, the measurement models were modified by means of covarying different parameters, treating other parameters as free parameters, and deleting relationships that had low regression weights as suggested by Amos. The research reported on chi-squared (χ^2), root mean square error of approximation (RMSEA), comparative fit index (CFI), goodness-of-fit index (GFI) statistics, and standardised root mean square residual (SRMR). According to Kline (2015), there are a number of fit indices that one can use; however, since there is no agreed standard number of fit indices to be used, studies should use at least three, provided the following mandatory ones are included: chi-squared (χ^2), CFI, and RMSEA. In addition to the mandatory ones, the research also incorporated GFI and SRMR. Therefore, this research reported on five fit indices. Table 5-4 shows a summary of each of the five fit indices and their threshold values as extracted from Arbuckle (2014).

Table 5-4: Fit indices threshold values

Fit indices		**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification.
	df		
	χ^2/df		
CFI		CFI ≥ 0.950	Above the threshold; this shows good fit.
RMSEA		0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification.
SRMR		RMR ≤ 0.08	Below the threshold value; this shows good fit.
GFI		GFI ≥ 0.90	Above the threshold; this shows good fit.

It is important to note that each fit index has its own threshold that should be met for the measurement model to be classified as of good fit. Appendix I gives detailed information about each of the measurement models and the results of fit indices.

5.6.1 Summary of measurement models

In SEM, the first step was the measurement of individual constructs (latent variables) using measured variables (survey questions), which yielded measurement models for each construct (Hair Jr. et al. 2014). This section summarises these measurement models, with details of each presented in Appendix I. The second step incorporated the measurement models in a single structural model with path analysis that illustrated the relationship between constructs. This is provided in Section 5.6.2. The figures and tables for each construct and measurement model are provided in Appendix I. The measurement models of the latent variables consisted of observable variables that were measured by means of a five-point Likert scale. The sections below give a discussion of each measurement model based on fit indices, with reference to figures and tables in Appendix I, including the verdict on goodness-of-fit for inclusion in the final SEM model. The abbreviations assigned to the constructs are used throughout this chapter, including in figures and tables that illustrate the SEM model.

Testing of performance expectancy (PE) model

The results in Table I-1 showed that the fit indices CFI, SRMR, and GFI were the only indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2 and RMSEA). Taken together, the fit indices indicated that the model was not a good fit and needed improvement. In order to modify the measurement model so that it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. After a rerun, the modified measurement model showed a good model fit for all five indices.

Testing of effort expectancy (EE) model

Table I-4 shows that the fit indices CFI, SRMR, and GFI were the only indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2 and RMSEA). Even though more than half of the fitness test showed a good fit, a better model could be achieved by modifying the models that suggested modification. Table I-6 shows the extracted fit indices, and taken together, the fit indices indicated a good model fit.

Testing of social influence (SI) model

The results in Table I-7 showed that the fit indices CFI, SRMR, and GFI were the only indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2 and RMSEA). Taken together, the fit indices indicated that the model was not a good fit and needed improvement. After a rerun, the modified model became poorer than it had been before modification; therefore, the researcher reverted to the original model, as three out of five indices showed good fit.

Testing of facilitating conditions (FC) model

The results in Table I-8 showed that SRMR and GFI were the only fit indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2, CFI, and RMSEA). Taken together, the fit indices indicated that the model was not a good fit and needed improvement. The measurement model was rerun, and the fit indices taken together showed a good model fit for the modified model.

Testing of hedonic motivation (HM) model

The results in Table I-11 showed that three out of five indices showed good fit, while two indices suggested model modification. CFI, SRMR, and GFI were the indices that showed good fit, while χ^2 and RMSEA suggested model modification. After modification of the model, the fit indices indicated a good model fit.

Testing of price value (PV) model

The results in Table I-14 showed that only two models had a good fit, that is, SRMR and GFI; the rest suggested model modification. The χ^2 value showed degrees of freedom of zero. According to Kline (2015), when the degrees of freedom are zero, it means that there is no way to affirm or reject the model; it means that the data have no 'freedom' to vary, and there is no 'freedom' to conduct research with this data set. Therefore, this measurement model was not used in the structural model.

Testing of habit (H) model

The results in Table I-15 showed that none of the fit indices showed a good fit – hence, suggesting modification. In order to modify the measurement model so that it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. The measurement model was rerun, with the resulting modified model showing a good model fit.

Testing of behavioural intention (BI) model

The results in Table I-18 showed that three models had a good fit, that is, CFI, SRMR, and GFI, while the other two suggested model modification. The χ^2 value showed degrees of freedom of zero. As mentioned earlier, when the degrees of freedom are zero, it means that there is no way to affirm or reject the model (Kline 2015). It means that the data have no 'freedom' to vary and that there is no 'freedom' to conduct research with this data set. However, because the construct BI was a mediator of several variables from the original UTAUT model, this model could not be rejected; therefore, the research used it as is in the structural model.

Testing of usability-learnability (UL) model

The results in Table I-19 showed that two fit indices – SRMR and GFI – out of the five measure-fit indices showed a good fit. Three of the fit indices, namely, CFI, RMSEA, and χ^2, suggested model modification. After treating the identified modification indices as free parameters, the measurement model was rerun, and the fit indices indicated a good model fit.

Testing of usability-user suitability (UUS) model

The results in Table I-22 showed that only two models had a good fit, that is, SRMR and GFI; the rest suggested model modification. The χ^2 value showed degrees of freedom of zero. When the degrees of freedom are zero, it means that there is no way to affirm or reject the model. Therefore, the measurement model for UUS was not used in the structural model.

Testing of usability-satisfaction (US) model

The results in Table I-23 showed that two fit indices – SRMR and GFI – out of the five measure-fit indices showed a good fit. Three of the fit indices, CFI, RMSEA, and χ^2, suggested model modification. In order to modify the measurement model so that it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. After a rerun, four out of five indices showed a good model fit. RMSEA was the only model fit that was slightly below the minimum of the threshold required. Considering the complexity of SEM, achieving four models of fitness out of the five required was acceptable; hence, no further modification was done.

Testing of usability-availability (UA) model

The results in Table I-26 showed that only GFI out of the five measure-fit indices showed a good fit. Four of the fit indices, namely, CFI, SRMR, RMSEA, and χ^2, suggested model modification. The measurement model was rerun, and three out of five indices showed a good model fit. RMSEA and χ^2 were the two model fit indices that were out of range – hence, suggesting further modification. It is important to note that, after accepting such model fit, when the measurement models are put together to form the structural model, if the structural model does not fit and requires further modification by deleting some constructs or construct items, then measurement models such as that of UA will be the first to be considered for deletion.

Testing of usability-errors (UE) model

The results in Table I-29 showed that GFI and SRMR out of the five measure-fit indices showed a good fit. The CFI, RMSEA, and χ^2 fit indices suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and four out of five indices showed a good model fit. Only RMSEA suggested model modification. However, when the measurement model of RMSEA was rounded off to the nearest two decimal places, as it was in the threshold, its value became 0.05, which was equal to the minimum of the RMSEA threshold; hence, the RMSEA was accepted as showing good fit.

Testing of usability-help and documentation (UHD) model

The results in Table I-32 showed that GFI and SRMR out of the five measure-fit indices showed a good fit. The CFI, RMSEA, and χ^2 fit indices suggested model modification. The measurement model was rerun, and four out of five indices showed a good model fit, with the exception of χ^2, which suggested model modification. The researcher decided against modifying the model for χ^2, as that could result in both χ^2 and RMSEA not fitting. Therefore, in order to achieve maximum fit, the researcher accepted the modified model.

Testing of security (S) model

The results in Table I-35 showed that GFI and SRMR out of the five measure-fit indices showed a good fit. Three of the fit indices, CFI, RMSEA, and χ^2, suggested model modification. After treating the identified modification indices as free parameters, the measurement model was rerun, and the modified model showed a good fit.

Testing of privacy (P) model

The results in Table I-38 showed that only SRMR out of the five measure-fit indices showed a good fit. Four of the fit indices, GFI, CFI, RMSEA, and χ^2, suggested model modification. The measurement model was rerun, and the modified model showed a good fit.

Testing of system usability scale (SUS) model

The results in Table I-41 showed that none of the fit indices showed a good fit – hence, suggesting modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and all indices showed a good model fit.

5.6.2 The online banking adoption and use structural model

Overall, the research drew 17 measurement models based on the constructs that were investigated, and 15 measurement models out of the 17 showed good fit, except for the price value (PV) and usability-satisfaction (US) models. Therefore, the online banking adoption and use structural model consisted of the 15 measurement models discussed earlier. The overall SEM is presented in Figure 5-2, which is essentially a path diagram that includes not only the observed variables, but also the latent variables. In the figure, latent variables (shown as a circle, with the variable abbreviation in capital letters – PE) were measured by means of the observable variables (shown by a rectangle, with the latent variable abbreviation in capital letters and lower-case letter numbering – PEa). Thus, the SEM diagram incorporated all the measurement models presented earlier, except PV and US. These measurement models consisted of all the initial theoretical framework concepts identified earlier from UTAUT2, usability, and security.

Figure 5-2 presents the overall SEM structural model, which includes 15 out of the 17 measurement models that were found to be a good fit in the previous section. The measurement models that showed good fit implied that those variables contributed to the overall model to explain the users' behavioural intention towards adoption and continued use of online banking. A simplified explanation and final structural model are provided in Figure 5-3. After the structural model was found to fit, the relationships that existed among constructs, between constructs and indicators, and among indicators themselves were analysed. Table 5-5 shows a summary extract from the Amos output for the standardised significance levels obtained after running the structural model. These levels showed the hypothesised relationships among the latent variables forming the underpinning effects on online banking adoption and acceptance. In order to determine the significance of the hypothesised relationship, Hair Jr. et al. (2014) recommend that a threshold of ± 1.96 be obtained for the values of the critical ratio (CR). This means that, for a hypothesis to be significant or supported, its constructs should have a critical ratio value that is greater than ± 1.96.

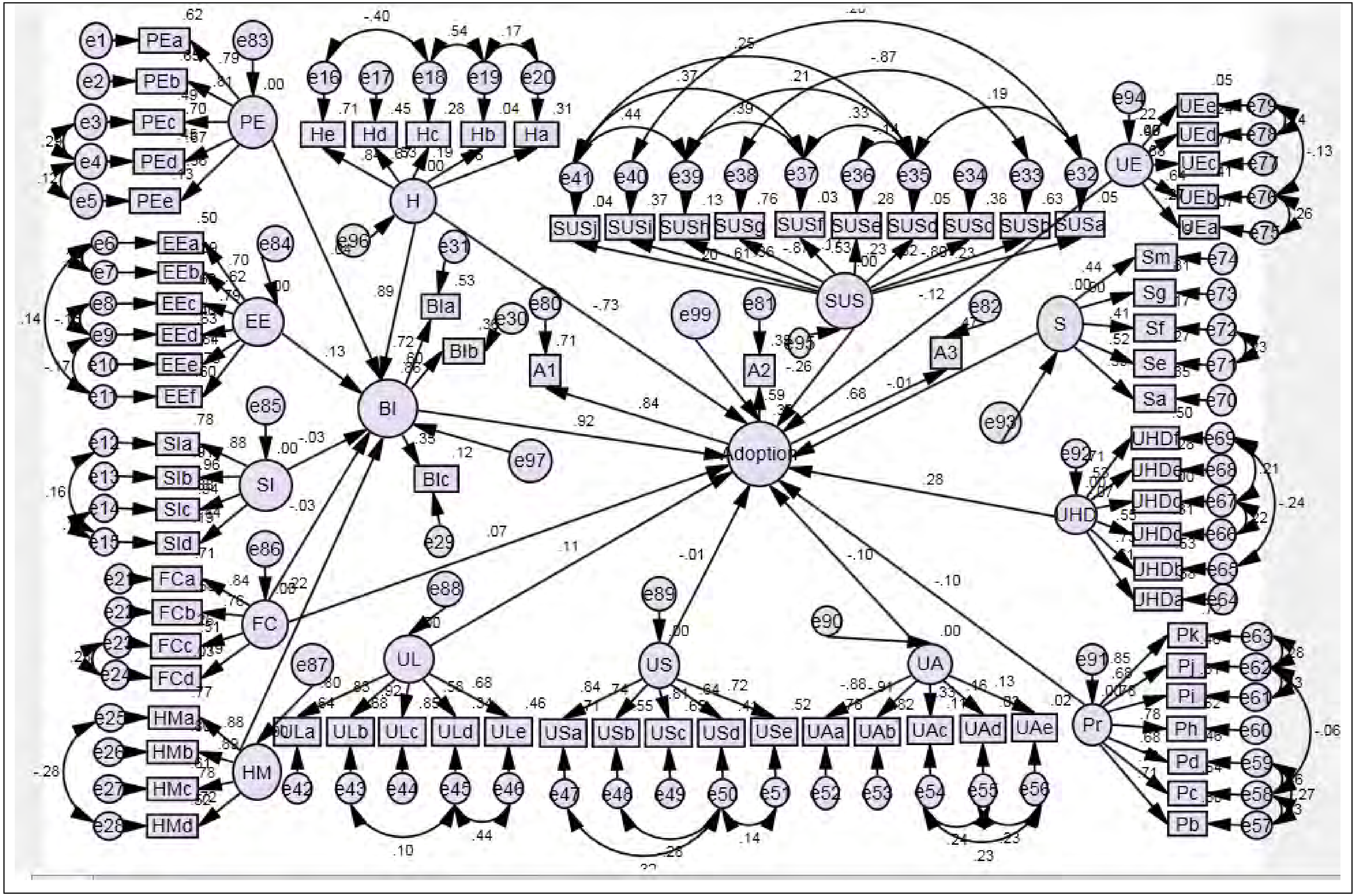


Figure 5-2: Structural model of online banking adoption and use

A conclusion on the hypothesis regarding the path of the structural model with a value above the threshold can then be reached, being either supported or else not supported. In traditional regression analysis, the critical ratio is tested as a t-value used to give predicting power. The results of the hypotheses tests are illustrated in Table 5-5.

Table 5-5: Summary of the standardised significance levels of constructs

Hypothesis	Path			Estimate	SE	CR	P	Comment
H1	BI	←	PE	0.046	0.039	1.167	0.243	Not supported
H2	BI	←	SI	-0.018	0.023	-0.771	0.441	Not supported
H3	BI	←	H	0.649	0.045	14.570	***	Supported
H4	BI	←	EE	0.087	0.024	3.584	***	Supported
H5	BI	←	HM	0.136	0.025	5.479	***	Supported
H6	BI	←	FC	-0.043	0.072	-0.594	0.552	Not supported
H7	Adoption	←	UE	-0.408	0.189	-2.163	0.031	Supported
H8	Adoption	←	US	-0.011	0.079	-0.141	0.888	Not supported
H9	Adoption	←	UHD	0.276	0.051	5.457	***	Supported
H10	Adoption	←	P	-0.080	0.037	-2.163	0.031	Supported
H11	Adoption	←	UA	-0.520	0.298	-1.747	0.081	Not supported
H12	Adoption	←	S	-0.018	0.056	-0.322	0.748	Not supported
H13	Adoption	←	UL	0.169	0.072	2.338	0.019	Supported
H14	Adoption	←	SUS	-1.041	0.279	-3.737	***	Supported
H15	Adoption	←	BI	1.733	0.364	4.760	***	Supported
H16	Adoption	←	FC	0.218	0.188	1.161	0.246	Not supported
H17	Adoption	←	H	-1.001	0.256	-3.916	***	Supported

Table 5-5 indicates that 10 out of 17 of the suggested hypotheses were supported. This is so because their CR values were above ± 1.96. Effort expectancy, hedonic motivation, and habit were found to have an impact on users' behavioural intention to use online banking, while performance expectancy, social influence, and facilitating conditions, contrary to UTAUT2, were not supported. In addition, habit, errors, learnability, help and documentation, SUS, privacy, and behavioural intention showed a direct influence on online banking adoption. These findings were presented in the final model, which included only the supported relationships, as illustrated in Figure 5-2.

Initially, there were 17 constructs, but two were dropped, as their measurement models did not pass goodness of fit, namely, price value and usability-user suitability. The remaining 15 constructs were included in the overall SEM structural model (Figure 5-2). The hypothesis testing of the remaining 15 constructs yielded the results as summarised in Table 5-5. These results further eliminated six constructs as having an explanatory impact on users' behavioural intention to use online banking and adoption of the service. The constructs not supported in the context of online banking adoption were performance expectancy, social influence, and facilitating conditions from the UTAUT2 model and satisfaction, availability, and security constructs.

5.6.3 Multigroup analysis with chi-squared difference test in Amos

In order to investigate the effect of moderating factors, the researcher conducted a multigroup analysis using Amos. Multigroup analysis in SEM is a method that allows one to compare multiple samples across the same measurement instrument or multiple population groups (for example, males versus females) for any identified structural equation model. Multigroup analysis in Amos also allows a researcher to test whether one's groups meet the assumption that they are equal by examining whether different sets of path coefficients are invariant. A number of methods can be used in multigroup analysis. This research used a chi-squared (χ^2) difference test in order to determine significant moderating factors regarding the hypothesised relationships.

According to Werner and Schermelleh-Engel (2009), frequent differences in model fit are subtler, and an objective criterion for a decision among competing models may be desired. Therefore, for this purpose, different models can be compared with regard to their model fit by performing a χ^2 difference test. Werner and Schermelleh-Engel (2009) postulate that a χ^2 test allows one to decide whether a given model fits significantly better or worse than a competing model.

A χ^2 difference test is meaningful and applicable only if the models in question are nested models; that is, one of the models could be obtained simply by fixing or eliminating parameters in the other model. This is supported by Arbuckle (2014), who says that, for nested pairs of models, Amos provides tables of model comparisons, complete with χ^2 difference tests and their associated *p*-values, when comparing models in those situations where one model just contains:

- an additional path in the structural model;

- an additional loading in a measurement model; or
- an additional correlation or covariance between latent variables, which the other model does not contain (where the parameter in question is fixed to zero).

In exploring the moderating effects, the researcher followed the following procedure:

1. The research made sure that all moderating variables were converted to dichotomous variables. Dichotomous variables are variables that are binary in nature; they only have two value possibilities, for example, gender, which has either male or female. Hence, variables such as age, experience, education, employment, ethnicity, and devices that were not naturally dichotomous variables were converted to dichotomous variables by means of recoding in SPSS. For example, the age of participants was grouped into two, the middle age-category being the cut-off point. Those with an age below the middle age-category were coded as a '1', and those aged above the middle were coded as a '2'. The procedure was followed for all the aforementioned variables. Table 5-6 provides an extract of the recoding performed on moderating variables; for a complete list, refer to Appendix J, Table J-1.

Table 5-6: Dichotomous recoding of moderator variables

#	Variable	Original coding	New coding
1	Gender	1 = Male 2 = Female	Used as is
2	Age	1 = Below 20 years 2 = 20-29 years 3 = 30-39 years 4 = 40-49 years 5 = Above 50 years	1 = Below 30 years (1-2) 2 = 30 and above years (3-5)
3	Experience	1 = Below 1 year 2 = 1-2 years 3 = 3-4 years 4 = 5-6 years 5 = Above 7 years	1 = 4 years and below 2 = Above 4 years
4	Education	1 = No formal education 2 = Matric 3 = Post-matric/diploma 4 = Degree 5 = Postgraduate degree 6 = Other	1 = No tertiary education (1-2) 2 = Tertiary education (3-6)

2. The research tested one variable at a time, by creating groups in Amos and assigning each group a subsequent group value.

3. The multigroup analysis feature was used, which would create different parameters automatically, including unconstrained and structural weights as well as structural covariances.
4. The research was only interested in unconstrained and structural weights; therefore, structural covariances were deleted.
5. The structural weights contained different structural weights for each relationship as in the model, which were given unique names. However, relationship b2_1 for Group 1 was forced to be equal to b2_2 for Group 2.
6. Next, the estimates were executed, and the output results were read under model comparison.
7. The model comparison gave results for the χ^2 test, and the focus statistics were the *p*-value, which ought to have a value less than 0.05 to show that there was a difference between the two groups. When the *p*-value was greater than 0.05, it meant that there was no difference among groups. It is important to note that this kind of moderation takes place at model level. However, this research hypothesised a moderation effect on specific relationships.
8. To test for moderation on a specific relationship, it was necessary to constrain the hypothesised relationship, while the rest of the relationships were treated as free parameters. To do this, all other relationships from structural weights were removed, except for those hypothesised.
9. After constraining the identified relationship, the estimates were calculated, and model comparison results were interpreted, looking at the *p*-value.
10. If the *p*-value was below 0.05, it showed that there was a difference among groups; in that case, further analysis of the moderating effects that had more groups was conducted. If the *p*-value was above 0.05, there was no difference among groups and, hence, no moderating effects.
11. If the model comparison results showed that the *p*-value was less than 0.05, the research looked at the standardised estimates for each group and obtained the regression weights for each group. A higher value meant that it had a stronger moderating effect than the others did.

After applying the above-mentioned procedure up to Step 5, the analysis resulted in two models, one of which is given in Figure 5-3, which represents Group 1 based on Table 5-6 ‘New coding’ column. The Group 2 model, which is identical to the Group 1 model, is given in Appendix J. Path b2_1 is for Group 1 as shown in Figure 5-3, while path b2_2 is for Group 2. (See Appendix J.)

Group 1 (b2_1)

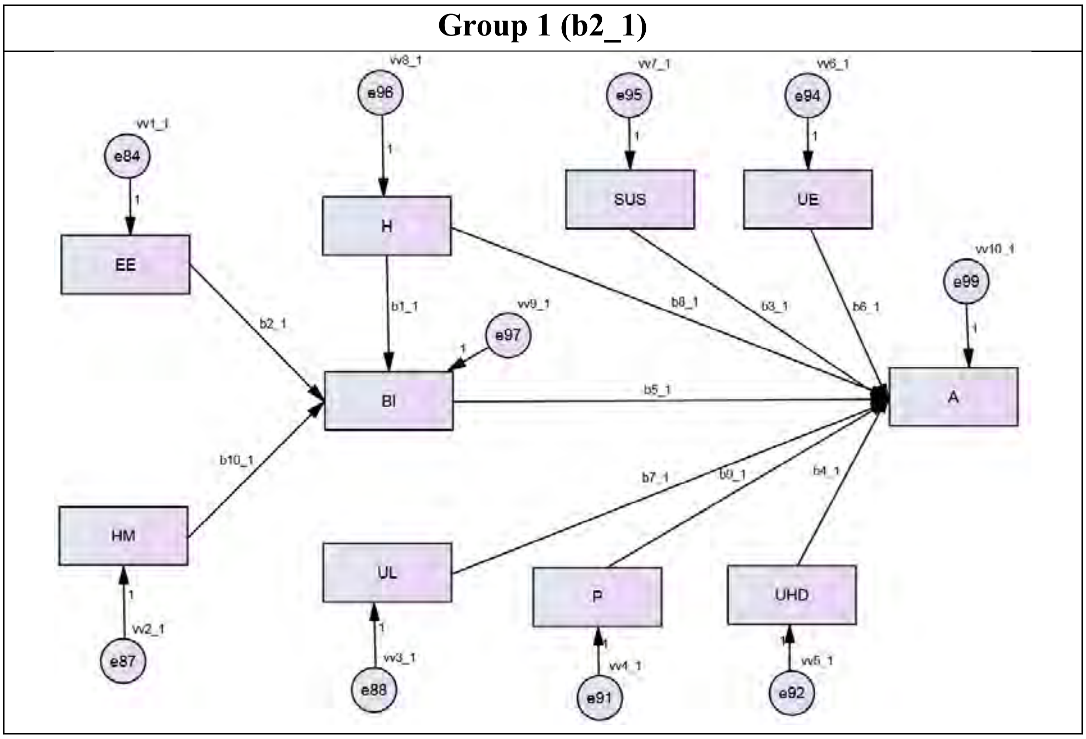


Figure 5-3: Dichotomous model: Group 1

The research repeated the above-mentioned procedure for all hypothesised relationships and moderating factors. Chi-squared comparison results and regression weights for each relationship and the moderating factors that were collected in the survey are presented in Appendix J, Table J-2. The results showed that only two moderating factors (experience and ethnicity) were significant and had moderating effects on three hypothesised relationships. Experience was found to have a moderating effect on the relationship between ‘adoption’ and ‘habit’, such that the effects were greater for less experienced users than for those with more experience. Furthermore, ethnicity was found to have moderating effects on the relationship between ‘behavioural intention’ and ‘hedonic motivation’, so that the moderating effects were greater for the non-African race than the African race. On the same note, ethnicity was found to have moderating effects on the relationship between ‘adoption’ and ‘habit’, as the effects were greater for the non-African race than the African race. The rest of the moderating factors (gender, age, education, employment, and device) were found to be insignificant.

5.6.4 Final structural model

The final SEM structural model based on all the analyses presented above resulted in the overall research model shown in Figure 5-4. The model showed the factors that influenced online banking adoption and behavioural intention to use the service. Habit exhibited an influence on both adoption and behavioural intention, while effort expectancy and hedonic motivation had an impact on behavioural intention. SUS, errors, learnability, privacy, and help and documentation all had a direct impact on adoption and behavioural intention.

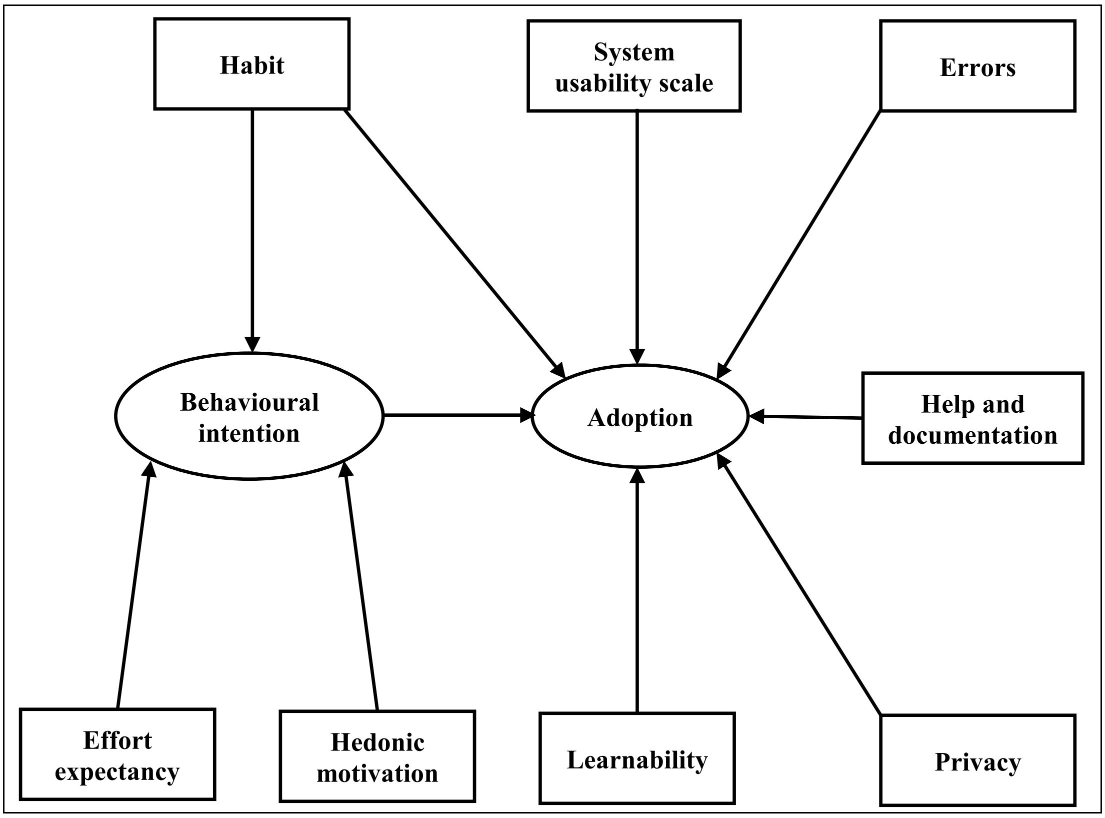


Figure 5-4: Final research model

Errors, learnability, privacy, and help and documentation were constructs that are also part of the STInfoSec framework (details provided in Chapter 7).

5.7 CHAPTER CONCLUSION

The chapter provided details of the quantitative method of the MMR design. The findings of SEM showed that 15 of the total of 17 measurement models had good fit for inclusion in the structural model. The excluded constructs were price value and user suitability, which were found to not have an effect on online banking adoption and continued use, contrary to the underlying UTAUT2 model. Furthermore, hypothesis testing using t-values rejected facilitating conditions, satisfaction, user suitability, and social influence as relevant constructs in the adoption and continued use of online banking. The resulting supported research model (Figure 5-4) consisted of eight constructs that had an effect on the adoption and behavioural intention to use online banking.

Three constructs, namely, habit, effort expectancy, and hedonic motivation were included in the final SEM model, as they were found to have an influence on user behavioural intention to use online banking. The SUS scale was found to be relevant in testing the usability of online banking applications. The STInfoSec framework included the following constructs from the structural model as principles: errors, learnability, privacy, and help and documentation. Chapter 6 provides details on qualitative data collection and analysis from the custodians of online banking to give a different perspective.

-- oOo --

CHAPTER 6 QUALITATIVE DATA ANALYSIS

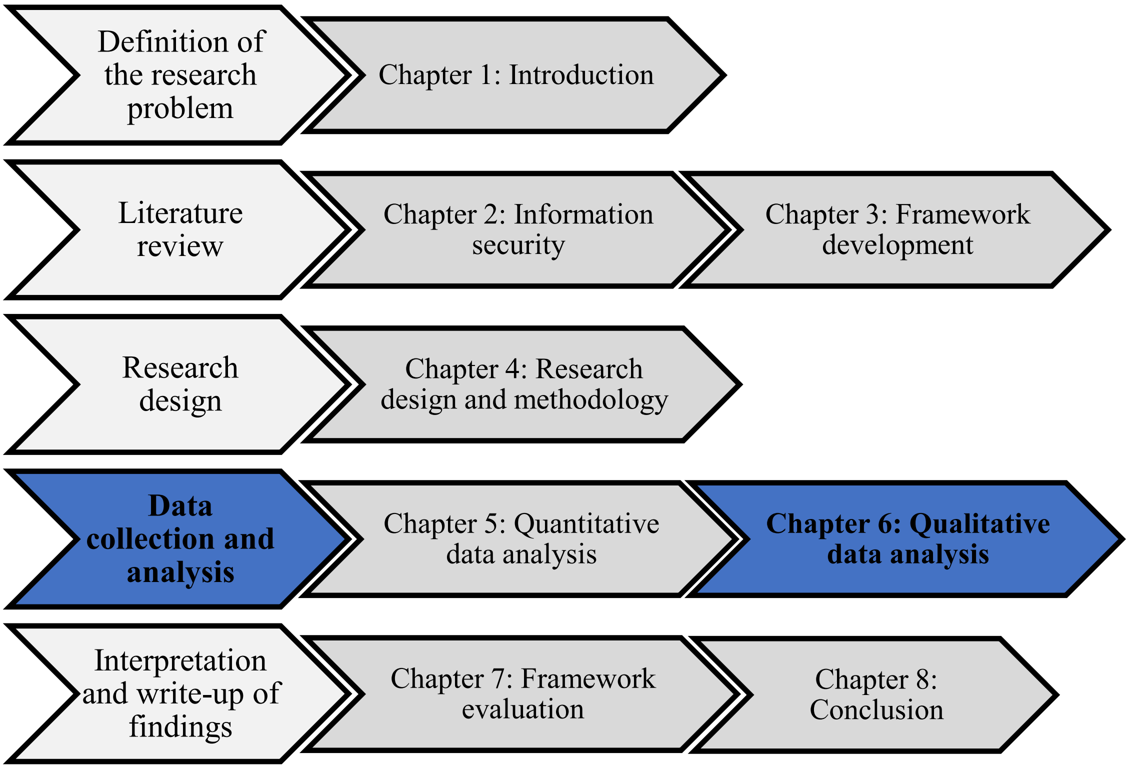

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 6-1: The research roadmap

6.1 INTRODUCTION

The purpose of this chapter is to present information on the qualitative data collection and analysis, explaining all decisions made in choosing data collection and analysis tools and techniques. The chapter first discusses the main sources of qualitative data and how the data were collected. This is followed by a detailed discussion of the chosen data analysis techniques (framework analysis), detailing how these were applied in this research based on the five stages of the method. The final stage of the framework analysis method linked the themes to *in vivo* coding, using participants' own words. Lastly, the chapter provides a final interpretation of the results based on the two data sets, linking the findings to the identified design principles and the STInfoSec framework. The combined findings of quantitative research (Chapter 5) and qualitative research (this chapter) formed the basis of the final design principles included in the STInfoSec framework presented and evaluated in Chapter 7.

6.2 DATA COLLECTION

The qualitative data for this research originated mainly from two sources: interviews with banking personnel working in security and digital channels and open-ended qualitative survey questions from an online banking users' survey. The sections that follow describe the sources of data analysed in this chapter.

6.2.1 Interview data

The objective of the interview data was to capture aspects considered pertinent by the custodians of digital channels in the design and development of online banking systems. Table 6-1 outlines the profiles of interview participants. The participants came from two of the four major banks in South Africa working with digital channels involving retail and corporate banking divisions.

Table 6-1: Interview participants' profiles

Participant	Gender	Position	Experience
P1	Male	Head: Enterprise Risk Management	10+
P2	Male	Chief Information Security Officer	1
P3	Male	Manager: Information Security	6
P4	Female	Head: On-boarding Self-Service Banking	10
P5	Male	General Manager: Electronic Payments	6
P6	Male	Performance and Security Testing	5

Participants came from different levels of management and had experience in different areas of InfoSec and digital channels in the banking industry. Semi-structured interview sessions were conducted at participants' workplaces between August and September 2016, each with an average duration of one hour. The questions covered a wide range of aspects, from general online banking service to legislation governing banking and online banking service. (See Appendix F.) Recorded interview audio data were transcribed by a qualified transcriber, yielding 30 pages of transcription text.

6.2.2 Survey data

The survey answered by online banking users included three open-ended qualitative questions that solicited additional information from respondents with regard to their experience with online banking systems. The first question asked what they liked most about the service; the objective of this question was to investigate the benefits of the service. Secondly, respondents were asked about their overall concerns regarding using online banking service, mainly to solicit drawbacks as perceived by current online banking users. This question attempted to gain insight into possible reservations about why adoption was lagging. Given that respondents were current online banking users, an in-depth investigation could only be obtained from respondents who had not yet enrolled for the service altogether (this was beyond the scope of this research). Hence, responses to this question only gave possible barriers based on current users. The third and last question asked for any additional comments, but this did not yield any further information that could not be classified into the first two questions.

6.3 FRAMEWORK ANALYSIS

There are a number of qualitative data analysis methods to choose from, and a researcher can select the one that best suits the research problem under investigation. The choices include ethnography, grounded theory, narrative analysis, content analysis, framework analysis, and historical research, to mention just a few (Schutt 2015). Ethnography is the recording and analysis of a culture or society, usually based on participant observation (Oates 2006); however, this was not the objective of this research. Grounded theory is a qualitative research method that seeks to develop a theory that is grounded in data (Turban et al. 2015), while narrative analysis is a qualitative data analysis approach that involves the interpretation and analysis of written or spoken words involving a story plot (Turban et al. 2015). Neither of these methods was suitable for this research, as the research was not either developing a theory or narrating a story.

Content analysis is a technique that looks for structures and pattern inferences in the text (Turban et al. 2015). Braun and Clarke (2006:79) define thematic analysis as "*a method for identifying, analysing, and reporting patterns (themes) within data*". Content analysis and thematic analysis are in the same group of qualitative analysis approaches, which also includes framework analysis, which seeks to identify commonalities and differences in qualitative data before drawing relationships between themes (Gale, Heath, Cameron, Rashid & Redwood 2013). Framework analysis was chosen mainly because it was aligned with the guidelines provided by Srivastava and Thomson (2009) on which research questions the technique helped to answer. A detailed motivation for, and description of, framework analysis use are outlined in this section.

Framework analysis is a qualitative data analysis approach that falls within the realms of thematic analysis or content analysis approaches. It focuses on commonalities and differences in qualitative data before zooming in on relationships between identified themes (Gale et al. 2013). Framework analysis was developed specifically for applied qualitative research. Srivastava and Thomson (2009:73) state that framework analysis is suited to "*research that has specific questions, a limited time frame, a pre-designed sample (e.g. professional participants) and a priori issues (e.g. organisational and integration issues) that need to be dealt with*". Ritchie and Spencer (2002:307) give guidelines on four types of research questions that framework analysis can help answer:

> *"Contextual: identifying the form and nature of what exists, Diagnostic: examining the reasons for, or causes of, what exists, Evaluative: appraising the effectiveness of what exists, and Strategic: identifying new theories, policies, plans, or actions".*

This research used framework analysis as the primary qualitative data analysis approach. Framework analysis was chosen for this research because it could help answer the following qualitative research questions:

Q3: What are the security designers' perceptions of users' security behaviour?

Q4: How can a socio-technical design approach be applied to improve the security and usability of online banking websites?

These questions fit into both the '*contextual*' and '*diagnostic*' categories as described above. The *contextual* aspect applied in that the questions investigated the existing perceptions of system designers regarding issues that might affect user behaviour during design decisions. The *diagnostic* aspect examined InfoSec environmental issues that existed that contributed to InfoSec problems and could help find solutions.

Framework analysis involves five key stages: *familiarisation, identifying a thematic framework, indexing, charting,* and *mapping and interpretation* (Ritchie & Spencer 2002). The five stages of framework analysis can be undertaken in a linear fashion either after all data collection or concurrently with data collection and analysis. A linear approach was chosen for this research, as qualitative data came from two different sources, namely, a survey and interviews; hence, analysis began after both sets of data were available for analysis.

Briefly, Ritchie and Spencer (2002) describe these stages as follows. *Familiarisation* requires the researcher to go through data by listening to audio tapes and reading transcripts to get the feel of the data as a whole. The second stage involves *identifying key issues, concepts, and themes* raised by research participants that form the basis of a thematic framework. This is followed by *indexing*, which refers to the linking of the identified themes to the transcription documents of interviews, commonly called coding in other qualitative data analysis approaches (Ritchie & Spencer 2002). Qualitative data analysis software packages such as ATLAS.ti make it easier to perform coding. *Charting* refers to the streamlining of the identified themes from all transcriptions. This process might include joining themes or eliminating certain themes. Finally, *mapping and interpretation* take place when all data has been charted according to key themes, thereby pulling together key characteristics for final interpretation of the whole data set (Ritchie & Spencer 2002).

Other scholars have developed a different number of stages of framework analysis; for instance, Gale et al. (2013) list seven stages: transcription, familiarisation with the interview, coding, developing a working analytical framework, applying the analytical framework, charting data into the framework matrix, and interpreting the data. Regardless of the number of stages one decides to apply, it is important to note that all activities of framework analysis are addressed in both approaches. The researcher decided to apply the original five stages as described by Ritchie and Spencer (2002). Framework analysis can be employed inductively, where themes are predominantly generated from participants' accounts, or deductively using a priori concepts from literature, or a combination of both (Gale et al. 2013). Given the MMR design of this research, a combination of both the inductive and deductive approaches was used to generate final themes for analysis. The details of these two approaches are provided in the stages sections. Figure 6-2 presents a diagrammatic representation of the framework analysis stages adapted to specific qualitative activities relevant to the current research and how the stages were applied in this study.

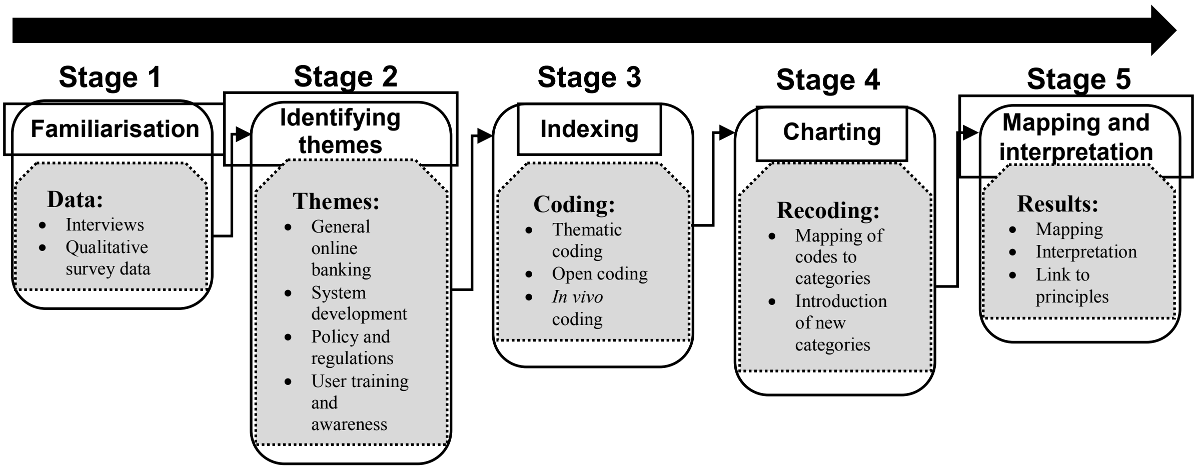


Figure 6-2: Application framework analysis (adapted from Georgsson & Staggers 2016)

The sections that follow outline the activities carried out by the researcher in each of the stages of framework analysis.

6.3.1 Stage 1: Familiarisation

For interview data, this stage involves word-for-word transcription of the interview audio files. Appendix K provides an excerpt of the interview transcript of one participant. The complete list of interview transcripts is available on a CD on request from the researcher. The researcher then reads these transcriptions and familiarises himself/herself with the content as provided by participants. Some scholars split transcription and familiarisation into two separate stages (Gale et al. 2013). In this research, both transcription and familiarisation constituted the first stage, based on the original framework analysis by Ritchie and Spencer (2002).

The transcription of interview audio files was performed by a professional language translator, yielding 101 pages with 30 000 words' worth of textual data. The researcher then listened to all interviews to verify the accuracy of interview transcripts, making corrections in instances where the transcriber had misunderstood the research field terminology, and verifying entries recorded as inaudible. Qualitative survey responses were extracted from the Google Forms responses spreadsheet into a Microsoft Word document. The researcher prepared both sets of qualitative data for computer-assisted qualitative data analysis software (CAQDAS). The ATLAS.ti software package was used.

6.3.2 Stage 2: Identifying a thematic framework

The familiarisation stage not only allows the researcher to gain an overview of the depth and richness of the data set, but also marks the beginning of the process of abstraction and conceptualisation (Ritchie & Spencer 2002). After going through the whole data set, the researcher had a holistic view and noted recurring themes, concepts, and key issues raised by participants. This process marked the second stage of identifying a thematic framework in framework analysis. Drawn from prior issues, this process raised themes on the basis of the framework, guided by the material giving rise to the interview questions and research aims.

This research investigated issues that security and digital channel designers of online banking systems perceived to be pertinent to a secure online environment. The issues addressed covered a plethora of areas from both designers' and users' perspectives. Using a semi-structured interview schedule, participants were free to address any specific areas during the interview sessions. These included online banking, legal aspects, system development, technology, user behaviour, as well as user training and awareness. The resulting insight helped identify areas of improvement in developing a service that would be both secure and usable.

The predefined thematic framework deductively identified concepts for investigation from the literature using thematic coding, while open coding after data collection constituted inductive theme generation based on participants' accounts (Gale et al. 2013). Table 6-2 provides the four themes that formed the predefined thematic framework based on semi-structured interview questions and a short description of each theme. These formed the basis of the interview schedule, as each theme was covered by an individual section in the interview schedule.

Table 6-2: Identifying a thematic framework

Theme	Description
General online banking	This covers general information about online banking, for example, costs, adoption incentives for users, and problem reporting channels.
System development	This theme involves system development decisions, including software development standards, internal versus external aspects, and composition of development teams.
Policy and regulations	The theme covers terms and conditions for the use of the service, including legally binding rules and regulations in the banking industry.
User training and awareness	The section covers initiatives for training and educating users about online banking functionalities and InfoSec awareness.

Indexing used thematic coding and open coding to generate the complete list of codes identified in framework analysis. *In vivo* coding was used for assigning pieces of text to the thematic framework, while new themes were also created from the data sets. This process is explained in detail under the indexing stage. Qualitative data interpretation inevitably includes coder bias (Cabrera & Reiner 2018). In this research, coder bias was mitigated by using the *in vivo* coding technique, which creates codes based on participants' own words (Belgrave & Seide 2018), and cross-referencing codes with quantitative data analysis in a mixed methods design (Cabrera & Reiner 2018).

6.3.3 Stage 3: Indexing

Indexing maps data sections from the transcripts to the identified thematic framework. This process involves coding when using CAQDAS, which does not analyse the data, but simply stores and organises it for easy access during analysis (Gale et al. 2013). Coding is the process of identifying these themes, concepts, or key issues and assists the researcher in organising and interpreting a data set (Given 2008). The identified codes are further differentiated or integrated into a smaller set of themes, relationships, and patterns to allow conclusions to be drawn from the data set. A code is a descriptive or conceptual label that is assigned to excerpts of raw data (Gale et al. 2013).

Thematic coding uses the identified thematic framework by assigning passages of text that are linked by a common theme or idea to the thematic framework concepts (Gibbs 2007). Open coding is a theme generation technique from qualitative data that allows the researcher to identify underlying concepts through data examination; in other words, there are no predefined themes for which the researcher looks in the data (Wolfswinkel, Furtmueller & Wilderom 2011). In this study, thematic and open coding both used *in vivo* coding to assign passages of text to the thematic framework codes (in thematic coding), and new codes missing from the thematic framework were created (in open coding).

In vivo coding is a coding technique that assigns a label to sections of data using a word or phrase from the participants' own words (Saldaña 2016). The code names essentially come from the text being coded, and the technique can be used in any type of coding of text data. *In vivo* codes allow the researcher to remain true to the data (Ritchie & Spencer 2002). Table 6-3 shows a detailed view of codes generated from both interview and survey data sets through *in vivo* coding. The code names are phrases extracted from participants' responses to either the interview questions or open-ended questions from the survey.

Table 6-3: Generated codes

	Interview codes		**Survey codes**			
No.	**Code**	**F**	**1. Likes**	**F**	**2. Concerns**	**F**
1	legislation and standards	75	convenience	310	security issues	285
2	security awareness	58	saving time	115	availability issues	44
3	system development	54	ease of use	83	trust and privacy issues	41
4	legacy systems	25	availability	55	limited functionality	36
5	security	25	satisfaction	36	UI changes	19
6	SABRIC	24	cost-effective	28	lack of awareness	12
7	breaches info-sharing	22	useful	18	technical limitations	11
8	client reporting channels	14	safety	15	not user-friendly	10
9	communication strategies	13			customer service	8
10	online banking training	13			costly	7
11	costs	13			inter-bank transactions	7
12	scaling down on branches	13			system design issues	6
13	security assistance	11			unclear error messages	5
14	terms and conditions	9			miscellaneous	17
15	digital channel awareness	8				
16	adoption incentives	8				
17	24-hour call centre	7				
18	competitiveness	7				
19	security breaches liability	6				
	TOTAL	**405**		**660**		**508**

The frequency (denoted by F) of each code in the data sets is also provided in the table. The coding was performed using ATLAS.ti, which allowed the researcher to assign varying sizes of words, phrases, sentences, or paragraphs to a code. The process of coding yielded 1 565 quotations across 40 unique codes from both sets of data. Themes aligned to the *in vivo* codes are provided in the next stage.

6.3.4 Stage 4: Charting

In this research, charting involved arranging specific data pieces that were indexed into a chart of themes (Srivastava & Thomson 2009). A mapping of predefined themes and generated codes from both interview and survey data sets through open coding resulted in the need to create additional themes, as some codes did not fit into any of the predefined themes. The process involved in the charting stage also provided a detailed analysis of themes. New themes were generated that combined interview data codes and survey data codes for common issues raised by both sets of participants.

The chart mapped themes to solicited codes generated from interview participants based on interview questions and unsolicited codes from survey respondents' general perceptions of the service. There was an overlap between areas of concern of both online banking users and custodians of the service. Table 6-4 provides the revised themes and comments based on the changes from the initial predefined themes given in Table 6-2.

Table 6-4: Revised thematic framework

Theme	Comments
System development	The same as the initial theme.
Information security	A new theme developed based on issues raised by online banking users and interview participants. It covers InfoSec- and privacy-related issues and general information about online banking, for example, costs, adoption incentives for users, and problem reporting channels.
Usability	A new theme based on the identified issues from interviews and survey responses.
Communication	Communication covers two-way communication strategies between the organisation and users for a variety of purposes, which include problem reporting, awareness initiatives, feedback, advertisements, etc. These issues were identified in interviews.
Regulations	The same as the initial theme.
Training and education	The same as the initial theme.
Benefits	These are benefits of the service as identified by online banking users through open-ended survey questions.

The revised thematic framework represented the final set of themes applicable in this research. Benefits were included to highlight the current views of online banking users, which, the researcher posited, financial institutions would need to take into account in providing digital solutions to their clientele. Table 6-5 presents the theme chart, with the respective codes provided in Table 6-3 for each theme.

Table 6-5: Theme chart

System development	**Information security**	**Usability**	**Communication**	**Regulations**	**Training and education**	**Benefits**
system development	security issues	user interface	client reporting channels	legislation	online banking training	convenience
legacy systems	trust and privacy issues	user experience	communication strategies	SABRIC	digital channel awareness	saves time
availability issues	security awareness	satisfaction	branch scale-down	terms and conditions	lack of awareness	ease of use
limited functionality	security	UI changes	24-hour call centre			availability
scalability	breach info-sharing		customer service issues			satisfaction
technical limitations	security assistance					cost-effective
not user-friendly	breach liability					useful
inter-bank transactions						safety
system design issues						
unclear error messages						

The researcher went through each code generated through open coding in Stage 3, assigning the codes to a specific theme based on the revised thematic framework.

6.3.5 Stage 5: Mapping and interpretation

Using a schematic diagram, Stage 5 involves the analysis of the main characteristics as outlined in the charts (Srivastava & Thomson 2009). The objective of the fifth stage in framework analysis does not involve issues that were raised by individual participants, but the collective perceptions from a group's perspective, capturing what the researcher has learnt (Lincoln & Guba 1985). This stage brings out the objectives of qualitative analysis, outlined by Ritchie and Spencer (2002) as "*defining concepts, mapping range and nature of phenomena, creating typologies, finding associations, providing explanations, and developing strategies*". Supported by quotations from participants, the researcher provided data interpretations, also in conjunction with previous findings in the literature and extant theories (Creswell & Creswell 2017). A more detailed presentation of this stage follows.

6.4 MAPPING AND INTERPRETATION

The main objective of qualitative findings in this research was to assist in developing a framework for secure and usable InfoSec applications, particularly the identification of usable security design principles for an online banking system. The themes were a set of key areas of online banking that needed to be addressed in development of the service, as identified by the research participants (both from the survey and interviews). The principles included concepts identified from the literature and included for investigation in the survey, as well as others raised by interview participants. These were evaluated in the final STInfoSec framework presented in Chapter 7. They were included in Figure 6-3 for illustration purposes and for their relationship to the identified themes in order to give an idea of the theme under which they could be addressed.

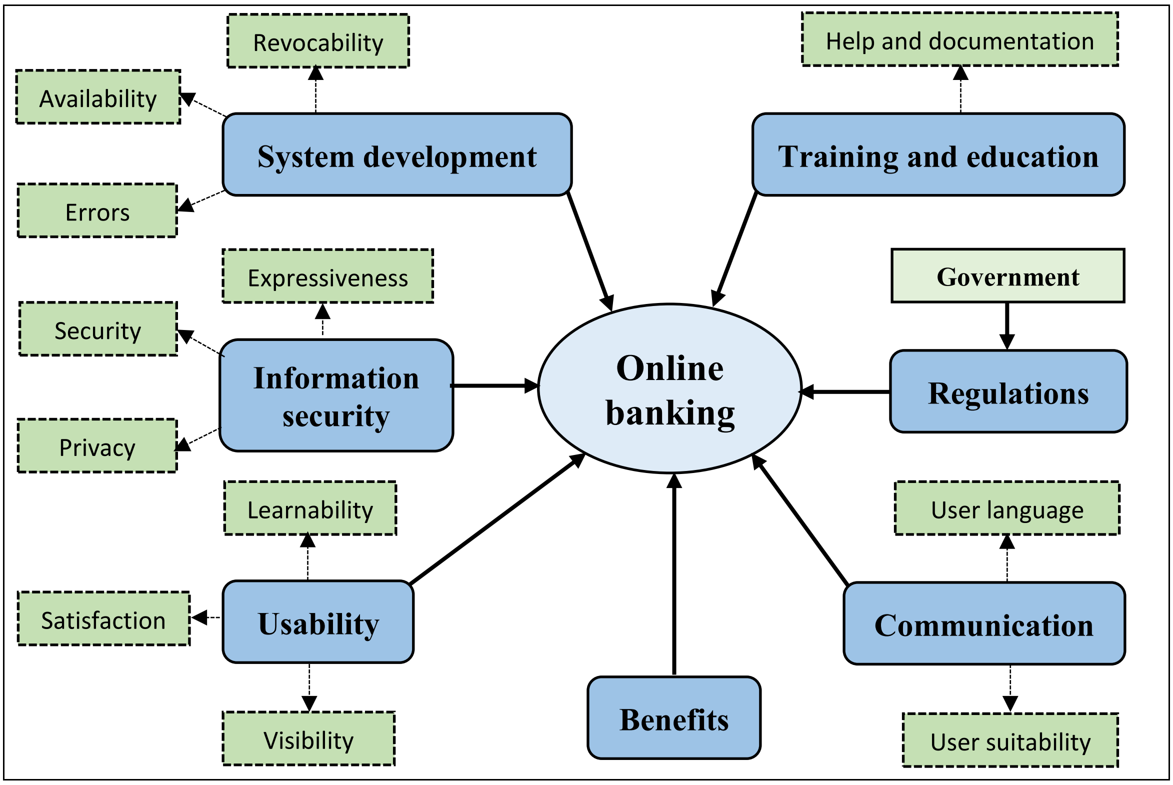


Figure 6-3: Mapping of themes and principles

The themes are in rectangles with solid lines (derived from Table 6-5), while the principles are in dotted-line rectangles. The mapping of themes provided the foundation for the principles and checklist items included in the STInfoSec framework presented in Chapter 7. The sections that follow provide details of participants' accounts with regard to each theme.

6.4.1 Information security

Security, in general, and InfoSec, in particular, came through as the main concerns of both users and online banking custodians. Online banking users were worried about potential financial loss due to a compromised online banking profile through hacking, identity theft, phishing, fraud, and loss of personal information (privacy). Designers were worried about the same threats. Their main concerns related mainly to finding ways to make users more vigilant when performing online activities; hence, the banks already provide awareness information to users through multiple channels.

Regardless of these efforts, the success of these initiatives is determined by the total buy-in of the users, as they are at the entry point of the system and are generally regarded as the weakest link in the security chain. The main problem faced by banks, as highlighted by all participants, is that users already exhibit unsecure behaviour from a very young age through other aspects of life such as social media. Hence, it is generally too late and difficult to expect banks to change their clients' behaviour. Participant P3 suggested a solution to this problem: "*I think it is more of a general awareness problem and government structures must roll out awareness in general to uplift the whole country's online awareness, little pieces* [sic] *that can be played by different role players.*"

Complicated cyberattacks and risky user behaviour make banks hesitant to market (or claim) their systems as the most secure, since a compromise can occur through zero-day attacks or user negligence. Participant P2 pointed this out: "*Even though we may be adopting all of the latest security mechanisms in our applications, you are always at risk because hackers are always clever and will come up with new ways. Sometimes it is not the inherent security within the system that is compromised, but it is the users' behaviour that they compromise like for instance through phishing.*"

In developing systems, banks employ local and international best practices as prescribed by numerous boards. Although these recommendations are not compulsory, it is in the best interests of financial organisations to conduct risk assessments and comply, where necessary. Participant P1 pointed out the need to collaborate with industry leaders in the areas of organisational risk and InfoSec: "*We don't have formal arrangements with any third party that advise* [sic] *us on security. We have a close relationship with people like KPMG*[2] *and Deloitte and with people like the Credit Bureau and FICO (Fair, Isaac and Company) who actually have a lot of insight in these* [sic]."

6.4.2 Usability

Usability of information systems is critical for attracting and maintaining customer loyalty to online applications. On the issue of addressing security, usability, and UX, banks do performance testing and incorporate feedback from focus groups, clients, and other stakeholders during the development stages before rolling out a system to users. There are dedicated usability and UX members in development teams, as mentioned by participant P5: "*To ensure that is it* [sic] *consistent we apply the* [sic] *standards.*

[2] This was before the problems engulfing the accounting firm with regard to state capture.

Therefore, we have a centre of excellence for the organisation. It used to be in different areas, but we wanted to make sure that UX is consistent and standard; hence, there is a division that looks after that." Participant P2 also alluded to the importance of penetration security tests before launching applications: "*Before we launch it, to test the security of the system. So any client facing online application* [sic] *will go through that process.*"

The recurring problem in system development has been, and continues to be, that usability is considered a secondary goal. This was supported by participant P5, who emphasised the importance of first addressing security and then considering usability afterwards: "*We are dealing with such large amounts of money that you have to make sure that first and foremost you are secured on behalf of your clients and shareholders. So that is the first priority, then obviously the debate about usability, competitive advantage comes into play.*"

Participant P5 admitted that security practitioners were faced with a trade-off between security and usability goals: "*Security is one of those things ... so security is a trade-off. We can make security possible but not usable.*" Fortunately, the situation is improving, as the participant proceeded to point out: "*Look what's good, what's nice is that, you know, and as technology evolves there are better security systems that are more usable.*"

Online banking users, however, raised concerns that pertained to usability and UX, with a number of codes, which included system user-friendliness, frequent user interface changes, and unclear error messages. Users also raised problems such as system downtime, limited functionality online, and the delay in inter-bank transactions.

6.4.3 Training and education

Participants interviewed highlighted initiatives provided by banks to train and educate users. These included in-branch pamphlets, online security centre portals, billboards, and radio and television advertisements. Banks also provided in-house training sessions for corporate online banking clients, although this initiative was not available to retail clients. On the provision of training programmes for retail online banking clients, participant P1 said the following: "*We don't give a formal set of training documentation or offer them* [sic] *to come for training. However, we do put certain statements on the system where* *they can view Frequently Asked Questions (FAQ), which can help them with certain things.*"

For corporate clients, one bank provided detailed training material, as outlined by participant P4: "*When you use the wholesale channels, there is an operational manual, context sensitive help, FAQs, and demos are available when the sales people go out to take the clients through it.*" Most importantly, the look-and-feel of both retail and corporate digital channels needs to be consistent. This makes it easier for users to learn the user interface, as pointed out by participant P4: "*The logic there is if you use it in your personal capacity, if you later log on as a corporate user you kind of like know how to locate functions. Therefore, we believe that there is a large portion of learning and training that takes place through the actual front end. So, it needs to be learnable.*"

The awareness programmes are meant to educate and assist users by fostering secure user behaviour. Among other things, these include recommendations on system requirements that include up-to-date patching of operating systems, up-to-date antivirus software, free downloads of anti-phishing software, and information on the risks of sharing login credentials. These solutions still require users' actions for them to be effective. Participant P1 summarised this requirement: "*Anyway, we do have a lot of awareness on security especially with our customers as far as possible. It is not training them but it is* ***creating awareness at every contact point*** *where we believe we can, in some form or format. But it's never enough.*" For example, users still wrote passwords on sticky notes attached to PC screens, which participants P3 and P4 witnessed during their client site visits. The participants also shared the concern that clients still shared passwords, both in the retail and corporate environments.

SABRIC, in conjunction with banks and cash-in-transit companies, strives to create a secure environment, as highlighted in its mission statement (SABRIC 2018):

> "*To deliver measurable value to our clients through a team of specialists who consistently provide high quality support services and products, and to contribute to the reduction of bank related crime through effective public private partnerships. Together with our clients and public private partners we view crime reduction as a shared responsibility and collective priority.*"

The Banking Association of South Africa (BASA) is another organisation that provides awareness information to both financial institutions and their clients. BASA is a representative of the banking sector, mandated to engage in lobbying and influence policy for the sector. Compared to SABRIC, the association covers a wide range of areas, which include financial sector legislation, client complaint procedures, and fraud awareness, to name but a few (BASA 2018).

Training and education are not only limited to the security aspects of the system, but also involve system functionality. It turns out that bank clients conduct in-branch banking transactions that are available through online channels due to a lack of awareness regarding the capabilities of the online banking service. To this end, banks inform clients through awareness information inserted in electronic and monthly printed statements sent to them and through using mainstream advertising. Training and education address some of the fundamental aspects of system usability, which include learnability and memorability, to allow users to be able to use the system consistently the first time and on subsequent occasions. Hence, developers need to create applications that are easy to learn and provide detailed and accurate reference material in case users face challenges.

6.4.4 Communication

Another aspect closely linked to awareness initiatives is that of communication strategies. The interview participants highlighted a number of strategies used by banks to communicate with their clients, either to disseminate information or get feedback and queries from clients. For example, clients can report fraudulent activities in their accounts through online live messaging tools, feedback forms, email, and 24-hour-operated call centres. South African banks mainly provide 24-hour call centres for critical security-related incidents such as lost credit cards and ongoing phishing attacks.

Participants alluded to it being a huge challenge to make sure that clients read the information provided and made available, be it instructions, awareness messages, or legally binding documents. This is a challenge not only in online banking, but also in other applications that require user attention to the fine print. To improve this aspect, banks strive to make these documents as concise as possible. In most cases, accepting the terms and conditions is compulsory before proceeding to one's online banking profile, as

Participant P6 stated: "*People do not read them. However, when you sign up for the first time, you cannot go through unless you have read and understood and clicked on it.*" There are, however, no guarantees that clients actually read these documents before clicking on 'Accept' to proceed.

6.4.5 System development

One area that security and usability practitioners of online applications can address directly is that of system development strategies that take the inherent flaws in user behaviour into account. Interview participants mentioned that they followed standard software development strategies, which applied approved life-cycle stages. Business decisions such as availability of personnel skills, cost, and duration of delivering the product dictate the final decision on product development. Options include off-the-shelf solutions, versus in-house development, versus outsourcing to third parties. In some cases, a combination of the three options can be employed to resolve a system requirement, as long as the business case is made for that decision.

Participants alluded to the limitations imposed on financial institutions by the problem of legacy systems, mainly because most banks were formed through amalgamation of small banks, and these brought their own systems that needed to be patched to work as a whole. This created an integration problem among these disparate systems, as noted by participant P1: "*... the bank's philosophy has always been to be a fast follower rather than creating new things from scratch but integration has been a problem. We have too many systems and also a strategy to decommission duplicate systems that do the same thing and you have 1 rather than 10 and that the longer-term project* [sic]."

The need to replace legacy systems can arise from a couple of issues, namely, shortage of skills to manage the systems that run on 'obsolete' platforms and lack of scalability to provide new technologies. Unfortunately, owing to cost implications, banks have taken a measured and long-term approach to solving legacy system problem, with concurrent migration projects running to reduce the impact on business processes and budget allocations. Participant P1 stated the following: "*Each project is worth somewhere over and above R10 million+, so these are big projects that are all running concurrently to migrate to what we need and where we want to be doing business in the future.*"

Banks also consider feedback from clients on system functionality through suggestion boxes and other reporting tools online. A business case is evaluated for any suggestions to decide whether it is a viable and feasible suggestion or functionality to add to the system. One bank had a system that collected ideas on how to improve business processes from personnel and clients for consideration during system improvement decision-making. In this regard, participant P6 made this remark: "*So if you have an idea of how things can be changed or expedited. You are welcome to log that idea to* [sic] *the system; at the end of the year they will have to review all those ideas.*"

6.4.6 Regulations

Online banking, just as any other service in the country, does not operate in a vacuum. There is legislation that regulates the financial industry to ensure that industry players abide by the rules and regulations to protect all stakeholders against intentional or unintentional malicious activity. The participants were of the view that South African banks were doing a great job self-regulating to international standards in the absence of binding legislation in the cybersphere, although any shortcomings would be addressed through the incoming Cybercrimes and Cybersecurity Bill (Cybercrime Bill 2017), as the current Protection of Personal Information (PoPI) Act was insufficient to govern the ever-expanding cybersphere.

Participant P1 expressed the following view: "*There are still difficult legislative issues and then obviously with the privacy laws with PoPI and then the execution and implementation of that bill probably is still a challenge on* [sic] *everything. Is the legislation effective? I think probably not at this moment.*" The PoPI Act serves the purpose of ensuring that all South African institutions that collect, process, store, and share another entity's personal information conduct themselves in a responsible manner by holding them accountable (PoPI 2013). Participant P1 thought that the weaknesses of PoPI were not regarding the material of the Act, but were on the implementation side; it still did not cover all aspects in the cybersphere: "*Yeah, I think the gaps are more in* [sic] *the implementation practical implementation side. In addition, I think, I am not sure if there is legislative capability to legislate for* [sic] *new technology at this moment. I think there are definitely gaps.*"

Participant P3 pointed out that "[y]*our identity can be hacked from social media like by Facebook, now the user will always try to transfer the blame on to other people*". Hence, the client blames the bank for not protecting his/her account, while his/her personal information has been compromised elsewhere. Therefore, the regulations need to also put in place sufficient investigative capacity to ascertain the exact cause of security breaches.

Overall, the new Cybercrimes and Cybersecurity Bill is a step in the right direction, given the increasing sophistication in cybercrime, which is now operated by organised crime groups. Among other aspects, there is the issue of dispute resolution for online banking security breaches. Currently, with the prevalence of SIM-swap fraud, no one is taking responsibility, with cases ending up in court (Ismail 2017). A dedicated legal framework can assist in giving direction to policing and prosecuting cybercrime, which has gone digital and international.

6.4.7 Benefits

Regardless of all the issues raised by both the interviewees and survey respondents, there was an overwhelming appreciation of the benefits online banking offered to users. Among the most popular benefits were convenience and time-saving, followed by ease of use and system availability to conduct banking transactions at any time of the day. Other cited benefits included satisfaction with the service, cost-effectiveness, usefulness, and safety, compared to visiting a branch.

Banking personnel alluded to the need for banks to reduce the number of in-branch client visits by encouraging clients to use digital channels, as this decreased operational costs. South Africa is an emerging economy; hence, branch operations are still critical in maintaining visibility in a competitive banking environment. As such, the aim is to increase branches, contrary to developing economies where digital channels are mature and well received, to the extent of scaling down branch operations. This is exacerbated by the fact that the South African economy is still a monetary economy, where cash continues to be the main medium of exchange. Participant P5 summarised this point: "*No we won't move away from branches in the short term near future, will we prefer our clients use electronic channels? Absolutely. Because it is more convenient for them and for us at the end of the day, but South Africa is a cash-based economy.*"

Additionally, clients have unique queries that sometimes need face-to-face interaction or at least a telephonic conversation. Therefore, branches now provide telephone terminals for direct access to call centres for specialised advice that might not be provided by branch staff. Branches also provide free online banking terminals to assist clients at the branch with services available through online channels.

6.5 CHAPTER CONCLUSION

The qualitative data analysis gathered input from the custodians of online banking systems, which provided insight into the challenges faced in developing online applications in a socio-technical environment. The findings showed that a secure environment depended heavily on user behaviour for effective achievement of system InfoSec goals.

System development that provides the functionalities for users to accomplish tasks depends on a number of other aspects represented by the identified themes in this chapter. The themes from interview participants' responses gave insight into the perceptions of online banking system designers with regard to InfoSec user behaviour, including other related aspects that assist in developing secure and usable systems.

There were six interview participants from the banking industry, and the analysis was performed using the framework analysis technique, based on open-coded data. Using five stages of framework analysis, interview data and qualitative survey data went through the stages, from familiarisation, to identifying a thematic framework, to indexing (coding), to charting, and to mapping and interpretation. Initially, the thematic framework had four themes; then, after the charting stage in framework analysis, two additional themes emerged. The final six themes were mapped to the 12 principles for final interpretation in the last stage of framework analysis.

The analysis of interview and survey data reinforced some of the themes identified in the thematic framework that guided the interview schedule. These themes, together with newly emerging themes from open coding, then formed the basis for usable security design principles in the STInfoSec framework validated in Chapter 7.

-- oOo --

CHAPTER 7 FRAMEWORK EVALUATION

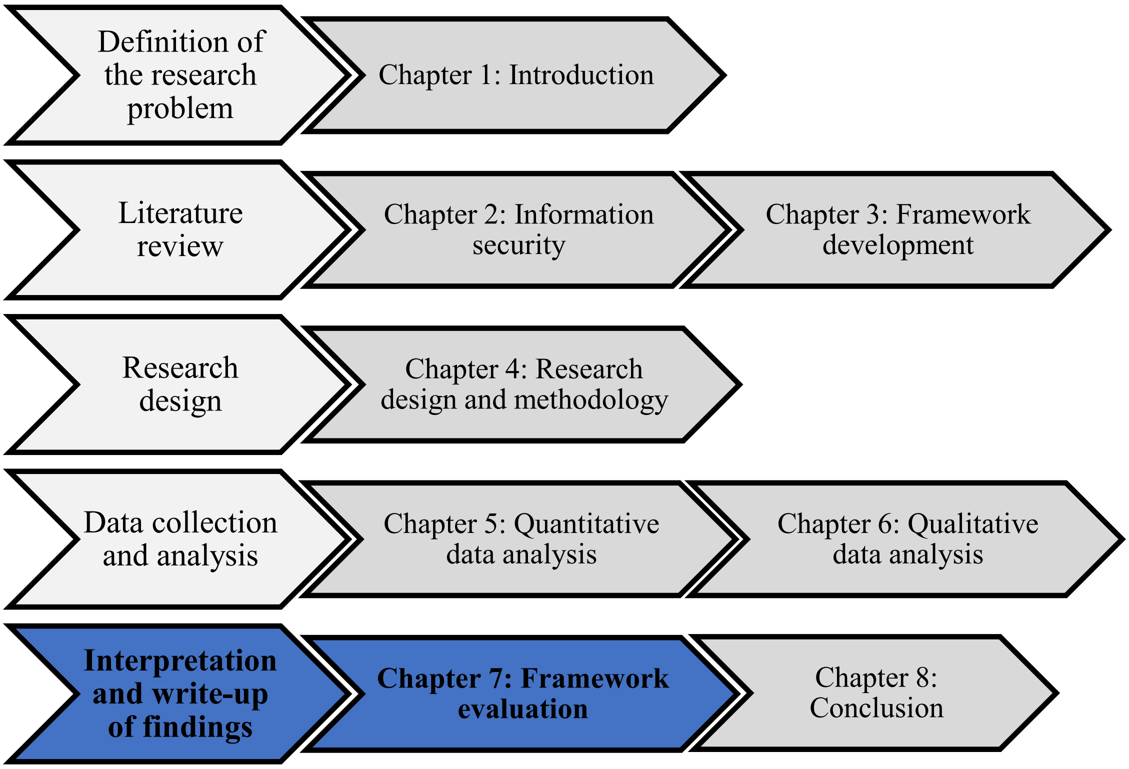

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 7-1: The research roadmap

7.1 INTRODUCTION

The previous two chapters presented quantitative and qualitative findings, respectively, of the MMR process followed in this study. Chapter 5 outlined the perceptions of users as they interacted with an online application that significantly relied on InfoSec to successfully fulfil its objectives. A number of hypotheses were developed and tested with the UTAUT model for technology adoption and continued use as foundation, based on 540 valid responses obtained from online banking users, resulting in the development of a structural model that incorporated constructs from usability, security, and UTAUT2. Chapter 6 presented the views of the custodians of online banking on challenges faced when users interacted with the service, highlighting the impact of user behaviour on interactions with online InfoSec applications, especially in this environment with highly sophisticated attacks and users who were not particularly computer and InfoSec savvy.

This chapter combines the findings of the previous two chapters in the development of a STInfoSec framework, which was the main objective of this research. The STInfoSec framework highlights the socio-technical aspects of InfoSec that aid in the development of online InfoSec applications. The framework essentially takes into consideration users' perceptions and expectations, as well as system designers' perceptions, in the development of such online applications. Given the increasingly social nature of InfoSec problems, emphasis on both the technical and social aspects of the problem is essential in creating applications that are both usable and secure. STInfoSec presents 12 usable security principles that assist in achieving usable online applications.

The chapter presents the evaluation process to validate the framework. The evaluation process was conducted using participants from academia and industry practitioners to obtain feedback from different perspectives for incorporation in the final framework.

7.2 EVALUATION PROCESS

The resulting usable security design principles from both the quantitative and qualitative analyses were evaluated by field experts from academia and the banking industry who had expertise in InfoSec, usability, and UX. The main objective of this process was to verify the significance of the usable security principles identified in the preliminary STInfoSec framework in addressing the problem of usable security in an online environment. Using the feedback from the evaluators, some of whom were participants in the qualitative interviews, the preliminary framework was finalised as a validated framework. The evaluation process involved the following steps.

7.2.1 Step 1: Development of checklist items

Checklist items were created for each of the selected principles, using a combination of the literature (previous studies), survey items, and the researcher's discretion, in the context of the case study (online banking). The 12 principles each had between five and nine checklist items. (See Figure 7-2 and Appendix L.) The evaluation tool was loaded into an online tool using Google Forms. The evaluation tool consisted of five sections, each of which is explained briefly.

Section A: Introduction – this section introduced the researcher and the background of the research topic to the participants, giving the context and insight into the evaluation process. It also explained the role of the evaluator and gave an estimate of the amount of time needed to complete the evaluation process. Section B: Consent form – the consent form gave a brief description of the ethical considerations of the evaluation process. The section outlined the steps to be taken to ensure ethical conduct and protect participants' privacy with regard to collection of personal information and evaluation responses. A detailed consent form and participation information sheets for the evaluation tool are provided in Appendix D.

Section C: Instructions – this part had information on how to complete the evaluation tool. The section explained the rating scale for checklist items of the principles. The scale was based on these four options: very important, important, moderately important, and not important. Evaluators were requested to provide additional comments, which were optional, at the checklist item and principle level. Section D: Biographical information – biographical information was collected for verification purposes and to ascertain the level of expertise of participants. This information included their full name (optional), gender, age, qualifications, and years of experience in relevant fields, to mention just a few. Section E: Checklist items – this final section consisted of checklist items for each of the 12 principles. It provided an introduction, with a rating scale, and reminded participants that they could provide additional comments.

7.2.2 Step 2: Identification of participants

The researcher identified and selected suitable participants based on the relevant expertise required to obtain valuable feedback. The identified expertise fields were usable security, InfoSec, usability, and UX. Experts from both academia and industry were invited to participate in order to obtain relevant knowledge from theoretical and practical perspectives. Participants from academia were researchers working in the above-mentioned fields, while industry practitioners were banking personnel who designed and worked with digital channels (the same as the interview participants in Chapter 6). Table 7-1 shows the profiles of the participants. There were seven participants, who included three from academia, two from private IT organisations, and two from two of the four major banks in South Africa (both of whom were also interview participants).

Table 7-1: Participants' profiles

Expert	Specialisation	Industry	Experience (years)
E1	Usability, UI design	Academia	15
E2	Usability	Academia	11
E3	Software testing	Private IT company	2
E4	Usable security, usability, UX	Private IT company	8
E5	Usable security, usability, UX	Bank	10
E6	Usable security, usability, UX	Bank	5
E7	Information security, usability	Academia	10

Five participants considered themselves to be at 'expert' level in at least one of the three relevant fields, namely, usable security, usability, and UX, with the intermediate and beginner levels having one participant each. Four participants had 10 or more years of experience in the relevant fields. The profiles showed that participants had sufficient experience and knowledge to provide valuable feedback in the evaluation process. The selection of participants from both academia and industry ensured the bridging of the gap between practice and theory by obtaining complementary views from diverse backgrounds and experience.

7.2.3 Step 3: Analysis of evaluation feedback

The evaluation feedback on the framework from participants (see Appendix M for a sample of responses) is explained in detail in section 7.4. The analysis also incorporated any changes suggested by participants regarding the levels of both principles and checklist items to improve the framework.

7.3 EVALUATION FINDINGS

The researcher sent 12 invitations to potential participants in the evaluation process, and seven responses were received. In line with Nielsen's recommendations of around five expert evaluators for heuristic evaluation (Nielsen 1994a), the researcher obtained seven evaluations for consideration based on the relevant expertise. This section presents the feedback as provided by participants through the online evaluation tool for each principle, including individual checklist items. Table 7-2 provides the average scores for each principle as scored by each evaluator (denoted by E1 to E7) to allow for a high-level analysis of the feedback.

Table 7-2: Average evaluation scores

#	Principle	E1	E2	E3	E4	E5	E6	E7	Average per principle	Summarised participants' comments
1	Visibility	3.5	4	2.7	3.7	2.7	3.3	3.7	**3.4**	The system has to be user-friendly and direct users to where to correct populated details.
2	Learnability	3.3	3.6	2.6	3.8	2.8	3.4	3.4	**3.3**	The learnability principle is very important, especially for the older generation.
3	Errors	3	3.6	3.4	3.1	2.5	4	3.5	**3.3**	There is still a need to hide some specific error information to avoid attacks that exploit too-detailed error messages. For example, a reply that username and password do not match is preferred to precisely which detail is incorrect to avoid brute-force attack vectors. Security is always a trade-off with user experience.
4	Availability	3	3.6	3	3.4	3	3.4	4	**3.3**	The new generation wants change.
5	Satisfaction	3.2	3	2.7	3.6	2.9	2.7	4	**3.2**	None.
6	Revocability	2.9	3.1	4	2.8	3	3.3	4	**3.3**	The provision of a cancelling option is necessary.
7	Expressive-ness	3	3.2	3	2.8	2.4	2.4	4	**3.0**	None.
8	User language	3.2	4	3.6	3	4	3	4	**3.5**	Again, too much information might be dangerous. We do not mention all the security capabilities of our systems to the end-user.
9	User suitability	2.8	3.3	2.5	2.7	2.8	2.7	4	**3.0**	It is important to always assume that the user is novice, especially in the information security field.
10	Help and documentation	3.1	4	3.4	3	3.9	3.2	4	**3.5**	None.
11	Privacy	3.5	4	3.9	3.8	3.8	3.8	4	**3.8**	None.
12	Security	3.6	4	3.7	4	4	4	4	**3.9**	None.
	Average per participant	**3.2**	**3.6**	**3.2**	**3.3**	**3.2**	**3.3**	**3.9**		

Additional comments or feedback provided by participants is presented as recommendations. These are meant to improve each principle in addressing the relevant aspects of usable security in system design. Using a four-point Likert scale, the participants rated the importance of each checklist item included in a principle to determine whether the system developers needed to consider it during system development. The Likert scale used the following scores: 1 = not important, 2 = moderately important, 3 = important, and 4 = very important.

Each participant's evaluation of individual principles based on scores for individual checklist items averaged above three (shown as 'Average per participant'). This indicated that all participants considered each principle to be at least 'important' for usable security design. In addition, the overall average for each principle across all participants (shown by the 'Average per principle' column) also indicated that the principle was considered by all participants to be at least 'important'.

Although, cumulatively, all principles scored above three ('important'), some individual checklist items were scored 'not important' and 'moderately important' by some participants. This was due to some reservations regarding specific checklist items in certain situations. For example, even if it is important to always provide users with detailed error messages, in some instances, too much information helps attackers. An example mentioned by one participant from a bank was not telling users whether the username or password as entered was incorrect, but just indicating that the information did not match, as this would significantly decrease the chances of a brute-force attack being successful.

One participant had reservations about system customisation to support both novice and expert users, stating the following: "*Always assume the user is novice especially in the information security field.*" This is contrary to suggestions by Nielsen (1995) to offer support for varying skills sets. The researcher, thus, concluded that, wherever possible, support for diverse skills levels was important. Only when such a design is not possible should the system default to novice-user settings. Hence, wherever possible, support for both user types is crucial.

7.4 VALIDATED STINFOSEC FRAMEWORK

The validated STInfoSec framework after the evaluation process is presented in Figure 7-2. The framework provides mapping of themes and principles in the socio-technical system, with some themes contributing to more than one component of the socio-technical matrix. For example, InfoSec and system development address aspects from both technology and tasks of the technical sub-system. In line with the original STS model, the four components are not independent from one another as they are all interrelated. The sections below briefly explain the four components of the socio-technical sub-systems in relation to Figure 7-2, with emphasis on specific usable security principles to contextualise the framework.

7.4.1 Structure

Structure is the first component of the social sub-system and consists of regulations, usability, and communications. Regulations are a critical aspect in the structure component. Although there are no principles directly linked to regulations, they form the fundamental building blocks of a regulated banking environment. The responsibility for formulating regulations falls in the realms of the government, in consultation with business (financial institutions). Financial institutions can also form a coalition, such as the SABRIC consortium, to share ideas on a variety of areas. The government seeks to create a balance between providing a business environment where organisations can operate and make a profit, while – at the same time – protecting and looking after the interests of citizens. Such regulations in the South African context include PoPI for the protection of clients' personal information that organisations collect and the incoming all-encompassing Cybercrimes and Cybersecurity Bill (Cybercrime Bill 2017). The Cybercrimes and Cybersecurity Bill aims to regulate offences committed in cyberspace, an area that currently has significant shortcomings in South African legislation. The structure component of the social sub-system also includes usability principles (visibility, learnability, and satisfaction) and communication-related principles, namely, user language and user suitability.

USABILITY

A. Visibility

1 The system shows the user the progress status during a visible delay in response time.
2 The system visibly shows the current selection/data input field.
3 The system clearly highlights the problem field with regard to error messages.
4 There is some form of feedback for every security-related action.
5 The system visibly shows the location of security-related options.
6 The help information for assisting the user is visible and easily accessible.

B. Learnability

1 The system provides easy-to-learn training material.
2 There is a quick-start guide to assist the user.
3 Security and non-security operations are easy to learn and use.
4 Security items have been grouped into logical zones, and headings have been used to distinguish among the zones.
5 The system presents security and non-security information in a standardised format.
6 Security options are selected by default.
7 The user interface makes it obvious which security items are currently selected.
8 The system protects users against making serious errors.

C. Satisfaction

1 The actual process of using the system is fun and enjoyable.
2 The most frequently used function keys are in the most accessible positions.
3 Security-related prompts imply that the user is in control.
4 Each individual security setting is a member of a family of security options.
5 The security mechanisms of the system provide a sense of protection to the user.
6 Colour has been used specifically to draw attention, communicate organisation, indicate status changes, and establish relationships for security- and non-security-related actions.
7 Users can personalise their own system, session, file, and screen defaults, such as the landing page.
8 The system fulfils its claimed capabilities.
9 The system completes unambiguous partial input in a data entry field.

COMMUNICATION

A. User language

1 The system allows the user to choose a preferred language.
2 Security actions and objects are named consistently across all prompts in the design.
3 Security information is accurate, complete, and understandable.
4 Security questions are stated in clear and simple language, where used.
5 The translation for preferred language selection is accurate.

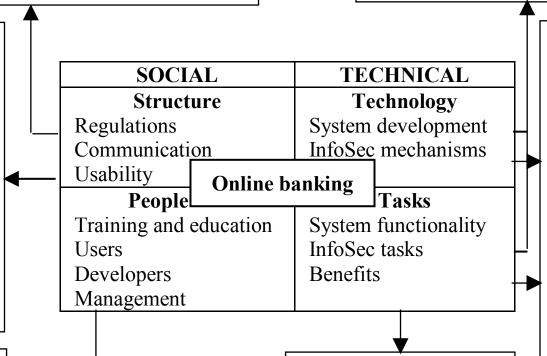
B. User suitability

1 Security information is accurate, complete, and understandable to all types of system users (experienced and novice).
2 Users can define and group their own synonyms for commands for easier access.
3 Users can navigate forwards and backwards within operations.
4 The system avoids the use of security and privacy jargon.

TRAINING AND EDUCATION

A. Help and documentation

1 The help function is visible; for example, a key labelled HELP or a special menu is provided.
2 The help function is easy to access, and return from, allowing users to resume their work from where they left off after accessing help.
3 The help function covers security- and non-security-related information.
4 The system provides an up-to-date security centre, with security training and awareness information.
5 The system provides a 24-hour help desk for critical security incidents.
6 The system provides a complete and accurate help function and a FAQs section.
7 The help and FAQs materials are searchable and grouped in logical categories.
8 The system provides detailed training and education material on how to complete basic tasks.
9 The system provides a search function for locating system functions.



BENEFITS

1 Convenience
2 Saving time
3 Ease of use
4 Availability
5 Satisfaction
6 Cost-effectiveness
7 Usefulness
8 Safety

SYSTEM DEVELOPMENT

A. Availability

1 The system is always available, with minimum and non-interruptive downtime.
2 The system makes sure that all system functionalities are available at all times.
3 Scheduled downtime is communicated in advance and scheduled during off-peak times.
4 The system limits the frequency of changes to the user interface.
5 Updates to the system's user interface do not result in users having to learn the system all over again.

B. Errors

1 System error messages are grammatically correct and accurate in stating the problem, with enough information for corrective measures/actions.
2 Security-related error messages inform the user of the severity of the error.
3 Menu items are arranged logically to prevent users making serious errors.
4 The system warns users if they are about to make a potentially serious error.
5 The system allows users to recover from errors quickly and easily.
6 The error messages of the system do not interfere with the users' work, whenever possible.
7 The system clearly asks for users' confirmation of serious and possibly irrevocable actions.
8 The system supports both novice and expert users and provides multiple levels of error message detail.

C. Revocability

1 Security options in menus make it obvious whether deselection is possible.
2 Users can easily reverse their security and non-security actions.
3 Prompts imply a necessary security action, with words in the message consistent with that action.
4 The system has been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions.
5 Users can cancel operations in progress.
6 There are 'undo' and 'redo' functions at the level of a single security action or for a complete group of security actions.
7 The system provides confirmation for actions that have drastic and possibly destructive consequences.
8 The system has a clearly marked exit.

INFORMATION SECURITY

A. Security

1 Critical transactions require out-of-band authentication such as an OTP/SMS.
2 The system initiates a session lock after a period of inactivity or on user request.
3 The system employs encryption techniques to prevent unauthorised disclosure of, and access to, information in storage and transmission.
4 The system enforces a limit on consecutive invalid access attempts by a user during a period of time.
5 The system implements an appropriate time-out logoff period.
6 The system encrypts passwords in storage and in transmission.
7 The system enforces password restrictions, such as complexity, length, expiry period, reuse, etc.
8 System password requirements are complex enough to avoid simple password-cracking attacks.

B. Privacy

1 The system asks for consent before collecting personal information.
2 The statements asking for user consent are written in clear and simple language that the user understands.
3 The system clearly states what personal information is collected and for what purposes it will be used.
4 The system requires users to confirm statements indicating that they understand the conditions of access.
5 The system asks for permission before distributing personal information to third parties.
6 The personal information collection and storage mechanisms comply with the data protection regulations of the country.
7 Protected or confidential areas are accessible using password authentication.

C. Expressiveness

1 Users are initiators of security actions rather than respondents.
2 The system correctly anticipates, and prompts for, the user's probable next security-related activity.
3 By looking, the user can tell the security state of the system and the alternatives for security-related actions, if needed.
4 The system clearly states its security capabilities.
5 The system clearly states the users' responsibilities in terms of security actions.

Figure 7-2: Validated STInfoSec framework

7.4.2 People

The people component consists of stakeholders in the online banking environment; these include users, developers, and management. These people play different roles in creating a secure and usable online banking service. Training and education make up the main theme in this component, as applicable to the assistance given to users to help them use the system effectively and efficiently through the principle of help and documentation. The theme of training and education also applies to the other stakeholders (developers and management) to assist them in carrying out their respective duties efficiently, although this falls outside the scope of this study.

7.4.3 Technology

The technology component in the technical sub-system consists of general system development and InfoSec mechanisms. System development ensures that the system addresses principles such as system availability, prevention of, and recovery from, errors, and revocability of transactions. In the context of InfoSec, the system provides technical capabilities to protect information assets in transit and in storage, such as system authentication, access control measures, and encryption mechanisms. Hence, the technology component essentially addresses actual development of InfoSec mechanisms that later provide the InfoSec tasks identified below.

7.4.4 Tasks

The second component of the technical sub-system, tasks, ensures that the system provides functionalities as expected by the users. These include actual online banking activities such as paying bills, managing accounts, and applying for new services. In addition, the system provides protection of personal and financial information using InfoSec mechanisms as provided by the system development component. These tasks are provided through the principles of security, privacy, and expressiveness. This component also includes the benefits offered by online banking tasks as identified by users through the qualitative section of the survey.

In the final STInfoSec framework, the principles include each of the detailed checklist items for easy application during the development process. The principles can also be used to evaluate an existing online banking application to check whether the service addresses usable security requirements. No further adjustments were made to the preliminary STInfoSec framework based on feedback from participants. However, recommendations were made and implications pointed out regarding principles and checklist items, as noted in Table 7-2. The proposed STInfoSec framework helps give direction on how exactly to develop usable security applications through a checklist that applies the identified principles.

7.5 CHAPTER CONCLUSION

The goal of this research was to assist in the development of online applications with a framework that applied a socio-technical view. Combined with UTAUT2, STS can be used to explain user acceptance and continued use of technology. UTAUT2 essentially predicts users' behaviour in deciding to adopt or reject a technology artefact. Hence, aiding the development of such artefacts through improving aspects that significantly make users reject a technology, such as a lack of usability and security, while optimising positive aspects, helps improve the adoption and continued use of such technology.

The preliminary framework was evaluated by seven evaluators from academia and the industry with a usability and InfoSec background. This process involved applying a heuristic evaluation method based on a checklist to each design principle to investigate the compliance of interface features with reputable usability principles. All 12 principles had above-average scores, and none of them were dropped from the final framework, shown in Figure 7-4. The principles were grouped into six identified themes.

To achieve this goal, firstly, the factors that affect user behaviour and encourage or prevent users from doing the right thing, even when they know the risks associated with non-compliance with InfoSec requirements, should be identified. Secondly, the design of InfoSec in online applications needs to identify the factors that make users feel inclined to bypass or ignore InfoSec mechanisms. For these reasons, the researcher assert that a socio-technical approach to InfoSec systems design can fulfil the goal of creating applications that are secure and usable, and the STInfoSec framework is one such approach. Chapter 8 concludes the thesis with an overall overview of the entire research.

-- oOo --

CHAPTER 8 CONCLUSION

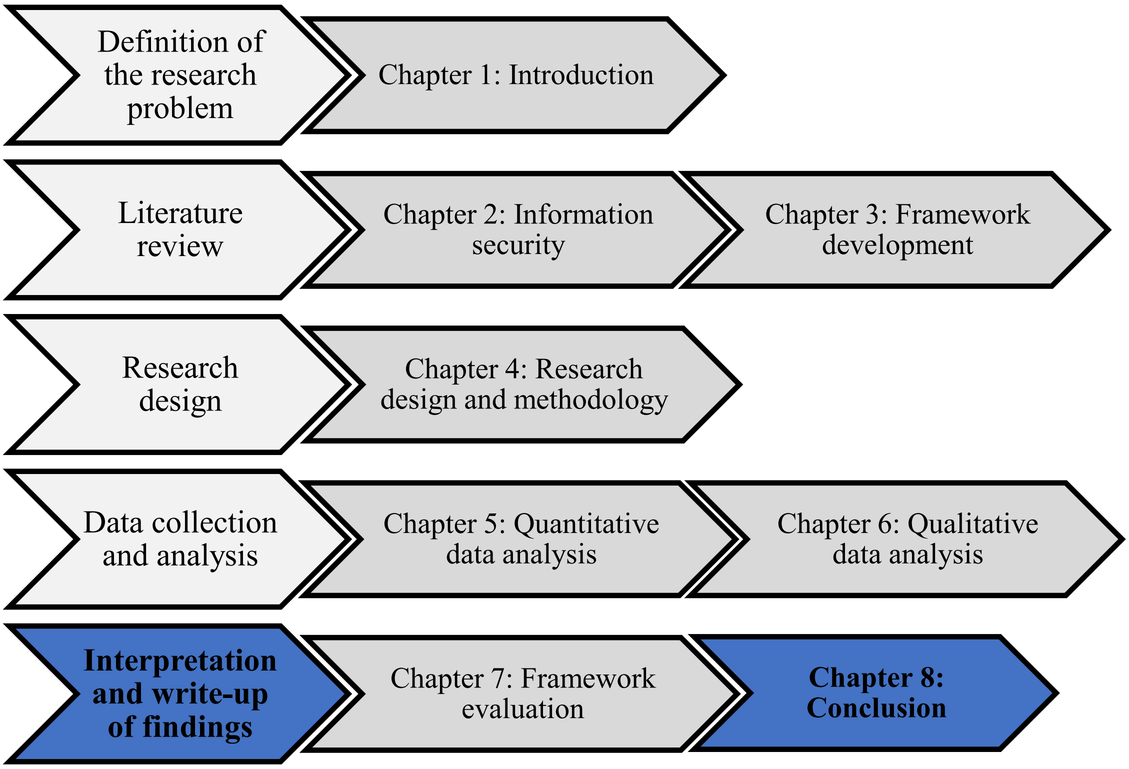

Definition of the research problem
Chapter 1: Introduction
Literature review
Chapter 2: Information security
Chapter 3: Framework development
Research design
Chapter 4: Research design and methodology
Data collection and analysis
Chapter 5: Quantitative data analysis
Chapter 6: Qualitative data analysis
Interpretation and write-up of findings
Chapter 7: Framework evaluation
Chapter 8: Conclusion

Figure 8-1: The research roadmap

8.1 INTRODUCTION

This chapter concludes the research by providing highlights that emanated from conducting this project. The research began with the main objective of developing a framework that assists in the development of secure and usable sensitive online applications based on the socio-technical approach. The framework was used to address usable security challenges in an online environment that relied heavily on conforming user behaviour by users who needed to be vigilant at all times to mitigate escalating online InfoSec threats. Unfortunately, it is difficult to rely on users' ever-changing behaviour; therefore, online application design must employ strategies that try to cater for user behaviour, taking into account inherent human limitations such as limited memory load.

The resultant product of this research was the STInfoSec framework that essentially considered InfoSec as a social problem that required a socio-technical approach for a holistic view of the problem. Using online banking as a case study, the STInfoSec framework presented 12 usable security principles for developing and evaluating this service in addressing usable security aspects, given the wide range of computer and security awareness levels of online banking users.

This chapter first presents a synopsis of the research questions and objectives that were outlined at the beginning of the study. This is followed by major contributions of the research to both the theoretical and practical body of knowledge. The limitations of the study are then presented, followed by potential further research areas to build on this research.

8.2 SYNOPSIS OF RESEARCH QUESTIONS AND OBJECTIVES

The researcher outlined research questions and research objectives to be answered and achieved, respectively, for a successful research project. This section provides a mapping of these research goals to how they were addressed during the course of the project.

The problem addressed in this research as mentioned in Chapter 1 was that **sensitive online applications (such as online banking) do not meet both information security and usability objectives**. The research proposed a framework to help in the development of secure and usable online InfoSec applications in the context of online banking. This led to the primary research question, formulated as follows: **How can information security-sensitive online applications be designed to be both secure and usable?** This question translated into the following primary objective of the study: **To develop a socio-technical framework that assists in the development of secure and usable sensitive online applications**. This section provides a synopsis of how sub-questions were each addressed in answering the research question and achieving the research objective.

8.2.1 Research question 1

What are the requirements for a socio-technical framework for the development of secure and usable information security online applications?

The design of a socio-technical framework requires an investigation of the socio-technical issues that need to be addressed by the framework. In the South Africa context, the adoption of online banking is considerably lower than the universal average, as cited in Section 2.10. This was the second motivation for choosing online banking as a case study. This question called for investigation and identification of factors that influenced user decisions in adopting or accepting a new technology. UTAUT2 is a widely used and accepted model for investigating technology adoption and continued use. The researcher contended that such factors, in the context of online

InfoSec applications, were socio-technical in nature. Therefore, for successful design, both the technical and social aspects needed attention. In light of this conclusion, the research postulated security and usability impacts as aspects that affected adoption, in addition to the conventional concepts identified by a unified model such as UTAUT2. The requirements were identified in the literature presented in Chapters 2 and 3. Chapter 2 highlighted online information security threats to which online users usually fell victim, while Chapter 3 identified usable security aspects for the design of online InfoSec applications.

Based on survey and interview findings, supported by a literature review, the research identified a group of 12 usable security design principles for online banking service. These principles were presented in a preliminary framework in Chapter 3 for validation and improvement into a final STInfoSec framework for the design of secure and usable online InfoSec applications.

Using SEM, the inferential part of the analysis investigated the significance of theorised constructs for overall adoption and acceptance of online banking in South Africa. The measurement models of SEM were computed for each construct before integrating all measurement models in the overall structural model. Two measurement models did not pass the goodness-of-fit tests (price value and user suitability), and these were excluded from the final SEM model. The hypotheses for the remaining 15 measurement models were tested, and a further six constructs were not supported. The final research model had nine constructs that were found to have a significant effect on online banking adoption and continued use. This was followed by multigroup analysis that sought to establish the effect of moderating factors on constructs based on dichotomous groups of respondents. Overall, the analysis found the effects on different groups to be mainly insignificant for most moderating factors, with the exception of two factors: experience and ethnicity.

8.2.2 Research question 2

How can a socio-technical framework for the development of secure and usable information security online applications be designed?

Chapter 3 provided a preliminary framework for the design of online InfoSec applications, presented in Figure 3-4. The framework involved the integration of usability, security, and UTAUT2 constructs that fed into the four components of a socio-technical model based on online banking service, culminating in the 12 usable security design principles. Using an MMR design, presented in Chapter 4, data was collected from both online banking users and developers. Chapter 5 presented quantitative data collection and analysis, while Chapter 6 reported on qualitative data collection and analysis.

SEM was applied to survey findings, highlighting the relationships among hypothesised constructs, moderated through a number of factors. This question was answered by the findings of the SEM model and multigroup analysis for moderating effects. The hypotheses included constructs from UTAUT2, InfoSec, and usability. The UTAUT2 model theorises concepts significant to individuals' intention to accept and continue to use a technology. In this research, the model was applied to explain the adoption of online banking service, which is an information system application that relies significantly on InfoSec mechanisms to protect users' financial and personal information. It was the contention of this research that the service was a socio-technical system that relied on both technical and social aspects for a secure environment; hence, two aspects that needed attention in systems design for the system to achieve its goals were added, namely, security and usability. The findings were presented in a structural model that explained user behaviour in online banking as a case study, as well as its relationship to service adoption and continued use. The results showed that usability principles, including SUS items, had a significant influence on users' behavioural intention and adoption of online banking. From an InfoSec point of view, privacy issues were found to have a significant impact, while security was not significant.

What transpired during interviews with participants was that online banking developers were aware of challenges posed by user behaviour in interaction with ISs, especially those with InfoSec mechanisms. The interview participants raised a number of issues that assisted in the design of usable security based on six themes: system development, InfoSec, training and education, usability, regulations, and communication. Specific issues were raised in each of these themes, as noted in Chapter 6, but the overwhelming theme alluded to the notion that a secure environment depended heavily on user behaviour for the achievement of InfoSec system goals.

8.2.3 Research question 3

How can a socio-technical framework for the development of secure and usable information security online applications be validated?

The preliminary STInfoSec framework that was developed in Chapter 3 and the data collected and analysed on the identified design principles for a socio-technical approach in Chapters 5 and 6 were validated in Chapter 7. The combination of the survey constructs of technology acceptance, information security, and usability of online applications yielded six main themes critical to usable security design in online banking. The themes were later mapped to the usable security design principles, showing areas where the principles might be addressed during system development. This mapping was provided in the final STInfoSec framework (Figure 7-2). The framework was validated using a heuristic evaluation method, based on checklist items (also included in Figure 7-2) for each principle, to address usable security problems. On the one hand, the checklist items can be used as a usable security evaluation tool for existing online banking systems. On the other hand, the principles can be used to evaluate existing online banking applications by applying the checklist items to identify and address usability problems. The evaluation was conducted using seven experts in the fields of usability, information security, and usable security.

8.3 CONTRIBUTIONS

The contribution of the research to the usable security body of knowledge was two-fold, namely, a theoretical contribution and a practical contribution; both contributed to the design of online InfoSec applications.

8.3.1 Theoretical contribution

Theoretically, the research contributed to the usable security body of knowledge by proposing a validated socio-technical STInfoSec framework for the development of online InfoSec applications. The research also hypothesised the impact of UTAUT2, InfoSec, and usability on adoption and continued use of online banking service. The STInfoSec framework views InfoSec as a social problem and presents 12 usable security design principles for the development of online InfoSec applications. The principles identified were specifically developed for online banking, but with minimum adaptation, these can be used to address other similar online applications.

Furthermore, the STInfoSec framework consists of checklist items that can be used as an evaluation tool of existing online banking and other related applications to investigate whether these applications satisfy usable security design requirements.

The research provided new insights into the use of MMR design in information systems to investigate usable security based on a combination of survey and interview data collection techniques in the context of online banking.

8.3.2 Practical contribution

The results of STInfoSec framework validation by field experts showed that the final framework could contribute to the development of secure and usable online banking applications. This would help create a secure online environment to allow the service to meet its intended goals from the points of view of both financial institutions and online banking users. A secure online environment encourages the adoption of the service, which, in turn, allows financial institutions to achieve a return on their investment in digital channels. This allows the banks to reach a large customer base, while decreasing costs by cutting back on branch operations and onsite staff. A secure and usable online banking service allows users to trust the service, thus encouraging adoption; most importantly, users feel safe in conducting a wide range of online banking transactions, thereby optimising benefits such as convenience, time-saving, and ease of use.

Apart from assisting in the development of usable security applications, the framework can be used to evaluate existing online banking applications using the checklist items validated for each principle. This process gives insight into the compliance of the current development process, while also simultaneously identifying areas of improvement.

8.4 LIMITATIONS

The research used online banking as a case study for the development of usable security of online applications. Hence, the application of the proposed framework to similar online applications might need small adaptations. The framework was limited to usable security principles, not extensive usability or information security principles in isolation. Therefore, principles that had no direct link to both usability and InfoSec were beyond the scope of this research project.

The research investigated adoption and continued use problems of online banking based on perceptions of users who were currently using the service. Although these users could help bring to light factors that made potential users hesitant to take up the service, a more in-depth investigation of adoption problems can be achieved by obtaining the perceptions of users not using the service. Furthermore, given the method of questionnaire distribution used, the researcher acknowledges the bias towards respondents that held higher education qualifications. This group of respondents was the most accessible to the researcher through online questionnaire distribution mechanisms.

Besides the identified and investigated usability principles, there are numerous other principles not addressed, not because they are not important, but because they were beyond the scope of the study. These include accessibility, which focuses on system accessibility to a wider range of users, including those with disabilities (Preece et al. 2015), and efficiency, which measures the speed with which users can achieve their goals accurately and completely after learning to use the system to some expert level (Rubin & Chisnell 2008).

Although the framework was evaluated by security and usability experts in both academia and industry, it was not tested in production settings. It has to be noted that, although the framework can assist in the development of a system, its application in a production setting will require that a number of other areas be addressed first. For example, external aspects such as cost and business goals often dictate the feasibility of any project in an organisation. Thus, the framework can assist in other initiatives currently in use to address development issues in usable security.

The framework proposed was not intended to solve problems associated with user behaviour regarding InfoSec, but it was meant to complement current proposed solutions in the field by contributing to the body of knowledge. Hence, even its implementation would need to take into consideration further aspects that might come from other fields and research studies and should not take place in isolation, as the InfoSec issue has since been identified as a social problem, with many facets that require a holistic socio-technical approach to finding solutions.

This holistic view requires the input of all stakeholders in the environment where information systems are developed and deployed, with emphasis on user-centred approaches. There is a need for the government to play a central role in educating citizens (especially at an early age) regarding the threats to InfoSec in a digital economy. This could possibly be done through the introduction of fundamental aspects in the school curriculum. There are countries already taking this initiative, with some degree of success (Cross, Shaw, Hadwen, Cardoso, Slee, Roberts, Thomas & Barnes 2016). In the context of Africa and other developing countries, Von Solms and Von Solms (2014) offer some suggestions, and one can only assume that such awareness initiatives are bound to raise awareness and mitigate cybersecurity threats.

8.5 FURTHER RESEARCH

This section provides information on further research opportunities in the area of this topic: usable security. These are suggestions that will assist in expanding the body of knowledge for secure and usable online applications.

8.5.1 Adoption

The perceptions of bank account holders with internet access, but not currently registered for online banking, will give an in-depth understanding of why these clients are not adopting the service. Hence, an investigation that involves only this group of respondents will assist in identifying the underlying factors that affect online banking adoption in South Africa.

8.5.2 Information security

InfoSec of online applications can be improved by using biometric technology, although there are still challenges. Research in this area is worthwhile to circumvent sophisticated online threats posed by organised crime organisations. Apart from mainstream use of biometric solutions, the usability of biometric technology needs further research for an improved InfoSec environment.

8.5.3 Usability

In terms of usability, further work could look at additional principles not included in this research. As noted in the literature review in Chapter 3, there are numerous usability and InfoSec principles that contribute to usable security design. Hence, an investigation of additional principles is necessary.

8.5.4 User experience

An investigation of in-depth UX of online InfoSec applications using online banking as a case study is warranted, given that we are currently moving beyond just the functionality and usability of online services for customer satisfaction, especially as users become technology savvy, and there are now a wide range of online services competing for users' attention. UX is becoming more of a need than a want to gain customer loyalty and retain customers in the digital environment.

8.6 CHAPTER CONCLUSION

This chapter concluded the research project by summarising the major aspects of the study, including giving a synopsis of the research questions and objectives. The chapter also highlighted the theoretical and practical contributions of the research, followed by research limitations and suggestions for further work.

In conclusion, InfoSec is increasingly becoming more complex, especially given the sophistication of attacks due to organised crime syndicates and the number of financial benefits associated with cybercrime. To make matters worse, more and more novice computer users are becoming participants in the digital world, with minimum or no InfoSec awareness of cyberthreats. Therefore, the concerted effort of all stakeholders is necessary to address the InfoSec problem in this digital environment in order to enable the development of holistic solutions. One aspect of such solutions is consideration of the involvement of human behaviour in the interaction of human beings with information systems. As such, this research is one step towards the needed holistic view of addressing InfoSec problems.

-- oOo --

REFERENCES

ACM SIGCHI (1992). *ACM SIGCHI Curricula for Human-Computer Interaction*, ACM, New York, NY.

Adapa, S. & Cooksey, R. (2013). 'Factors affecting consumers' continued use of internet banking: empirical evidence from Australia', *Australasian Journal of Information Systems*, 18*(1)*, pp. 5-31.

Ajzen, I. (1991). 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, 50*(2)*, pp. 179-211.

Alafeef, M., Singh, D. & Ahmad, K. (2011). 'Influence of demographic factors on the adoption level of mobile banking applications in Jordan', *Research Journal of Applied Sciences*, 6*(6)*, pp. 373-377.

Albert, W. & Tullis, T. (2013). *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*, 2nd ed., Morgan Kaufmann, Waltham, MA.

Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C. & Sanz-Blas, S. (2009). 'The role of consumer innovativeness and perceived risk in online banking usage', *International Journal of Bank Marketing*, 27*(1)*, pp. 53-75.

Alexa.com (2018). *The top 500 sites on the web*, available from: http://www.alexa.com/topsites, Alexa, San Francisco, CA, [last accessed: 25 January 2018].

Alsharnouby, M., Alaca, F. & Chiasson, S. (2015). 'Why phishing still works: user strategies for combating phishing attacks', *International Journal of Human-Computer Studies*, 82*(2015)*, pp. 69-82.

Althobaiti, M.M. & Mayhew, P. (2014). 'Security and usability of authenticating process of online banking: user experience study', *Proceedings of the 2014 International Carnahan Conference on Security Technology (ICCST)*, IEEE, Rome, 13-16 October, pp. 1-6.

Anderson, B.B., Vance, A., Kirwan, C.B., Jenkins, J.L. & Eargle, D. (2016). 'From warning to wallpaper: why the brain habituates to security warnings and what can be done about it?', *Journal of Management Information Systems*, 33*(3)*, pp. 713-743.

Anderson, J.M. (2003). 'Why we need a new definition of information security?', *Computers & Security*, 22*(4)*, pp. 308-313.

Angulo, J. & Wästlund, E. (2012). 'Exploring touch-screen biometrics for user identification on smart phones', In: J. Camenisch, B. Crispo, S. Fischer-Hübner, R. Leenes & G. Russello (eds.), *Privacy and Identity Management for Life. Privacy and Identity 2011. IFIP Advances in Information and Communication Technology, vol 375*, pp. 130-143, Springer, Berlin.

Antonius, R. (2013). *Interpreting Quantitative Data with IBM SPSS Statistics*, 2nd ed., Sage Publications, London.

APWG (2017). *APWG phishing activity trends report Q4 2016*, available from: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf, APWG, [last accessed: 25 January 2018].

Arbuckle, J.L. (2014). *IBM SPSS Amos 23 User's Guide*, 23rd ed., Amos Development Corporation, Crawfordville, FL.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F. & Kijewski, P. (2015). '2020 cybercrime economic costs: no measure no solution', *Proceedings of the 10th International Conference on Availability, Reliability and Security (ARES)*, IEEE, Toulouse, 24-28 August, pp. 701-710.

Barnum, C.M. (2011). *Usability Testing Essentials: Ready, Set... Test!*, Morgan Kaufmann, Burlington, MA.

BASA (2018). *The Banking Association of South Africa*, available from: http://www.banking.org.za/, BASA, Johannesburg, [last accessed: 25 January 2018].

Baxter, G. & Sommerville, I. (2011). 'Socio-technical systems: from design methods to systems engineering', *Interacting with Computers*, 23*(1)*, pp. 4-17.

Belgrave, L.L. & Seide, K. (2018). 'Grounded Theory Methodology: Principles and Practices', In: P. Liamputtong (ed.), *Handbook of Research Methods in Health Social Sciences*, pp. 1-18, Springer, Singapore.

Ben-Itzhak, Y. (2009). 'Organised cybercrime and payment cards', *Card Technology Today*, 21*(2)*, pp. 10-11.

Berger, A.N. (2003). 'The economic effects of technological progress: evidence from the banking industry', *Journal of Money, Credit and Banking*, 35*(2)*, pp. 141-176.

Bevan, N. (2008). 'Classifying and selecting UX and usability measures', *International Workshop on Meaningful Measures: Valid Useful User Experience Measurement*, IRIT, Reykjavik, 18 June, pp. 13-18.

Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F. & Savvides, M. (2015). 'Biometric authentication on iphone and android: usability, perceptions, and influences on adoption', *Proceedings of the USEC Conference*, Citeseer, San Diego, CA, 8 February, pp. 1-10.

Bhattacharyya, D., Ranjan, R., Alisherov, F. & Choi, M. (2009). 'Biometric authentication: a review', *International Journal of u-and e-Service, Science and Technology*, 2*(3)*, pp. 13-28.

Bidgoli, H. (2006). 'Internet basics', In: H. Bidgoli (ed.), *Handbook of Information Security: Key Concepts, Infrastructure, Standards, and Protocols*, pp. 3-14, John Wiley & Sons, Hoboken, NJ.

Biswas, D. & Biswas, A. (2004). 'The diagnostic role of signals in the context of perceived risks in online shopping: do signals matter more on the web?', *Journal of Interactive Marketing*, 18*(3)*, pp. 30-45.

Blanthorne, C., Jones-Farmer, L.A. & Almer, E.D. (2006). 'Why you should consider SEM: a guide to getting started', In: V. Arnold, B. Douglas Clinton, P. Luckett, R. Roberts, C. Wolfe & S. Wright (eds.), *Advances in Accounting Behavioral Research, Volume 9*, pp. 179-207, Emerald Group Publishing, Bingley.

Blyth, A. & Kovacich, G.L. (2006). *Information Assurance: Security in the Information Environment*, 2nd ed., Springer, London.

Bo, W., Zhang, Y., Hong, X., Sun, H. & Huang, X. (2014). 'Usable security mechanisms in smart building', *Proceedings of 2014 IEEE 17th International Conference on Computational Science and Engineering (CSE)*, IEEE, Chengdu, 19-21 December, pp. 748-753.

Bonneau, J., Herley, C., Van Oorschot, C. & Stajano, F. (2012). 'The quest to replace passwords: a framework for comparative evaluation of web authentication schemes', *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, IEEE, San Francisco, CA, 20-23 May, pp. 553-567.

Bonneau, J., Herley, C., Van Oorschot, P.C. & Stajano, F. (2015). 'Passwords and the evolution of imperfect authentication', *Communications of the ACM*, 58*(7)*, pp. 78-87.

Bostrom, R.P. & Heinen, J.S. (1977). 'MIS problems and failures: a socio-technical perspective, part I: the causes', *MIS Quarterly*, 1*(3)*, pp. 17-32.

Boyd, D. & Ellison, N.B. (2007). 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, 13*(1)*, pp. 210-230.

Braun, V. & Clarke, V. (2006). 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3*(2)*, pp. 77-101.

Braz, C., Seffah, A. & M'Raihi, D. (2007). 'Designing a trade-off between usability and security: a metrics based-model', *IFIP Conference on Human-Computer Interaction*, Springer, Rio de Janeiro, Brazil, 10-14 September, pp. 114-126.

Brooke, J. (1996). 'SUS – a quick and dirty usability scale', *Usability Evaluation in Industry*, 189*(1996)*, pp. 194-200.

Brown, S.A. & Venkatesh, V. (2005). 'A model of adoption of technology in the household: a baseline model test and extension incorporating household life cycle', *MIS Quarterly*, 29*(3)*, pp. 399-426.

Brown, T.A. (2015). *Confirmatory Factor Analysis for Applied Research*, 2nd ed., Guilford Publications, New York, NY.

Bryman, A. (2006). 'Integrating quantitative and qualitative research: how is it done?', *Qualitative Research*, 6*(1)*, pp. 97-113.

Cabrera, L.Y. & Reiner, P.B. (2018). 'A novel sequential mixed-method technique for contrastive analysis of unscripted qualitative data: contrastive quantitized content analysis', *Sociological Methods & Research*, 47*(3)*, pp. 532-548.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., Academic Press, Waltham, MA.

Chaudhry, J.A., Chaudhry, S.A. & Rittenhouse, R.G. (2016). 'Phishing attacks and defenses', *International Journal of Security and Its Applications*, 10*(1)*, pp. 247-256.

Cheng, T.C.E., Lam, D.Y.C. & Yeung, A.C.L. (2006). 'Adoption of internet banking: an empirical study in Hong Kong', *Decision Support Systems*, 42*(3)*, pp. 1558-1572.

Cheswick, W.R., Bellovin, S.M. & Rubin, A.D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA.

Chetty, M., Banks, R., Brush, A.J., Donner, J. & Grinter, R.E. (2012). '"You're capped" understanding the effects of broadband caps on broadband use in the home', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Austin, TX, 5-10 May, pp. 3021-3030.

Chiu, C.M., Wang, E.T.G., Fang, Y.H. & Huang, H.Y. (2014). 'Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk', *Information Systems Journal*, 24*(1)*, pp. 85-114.

Choo, K.K.R. (2011a). 'Cyber Threat Landscape Faced by Financial and Insurance Industry – Trends & Issues in Crime and Criminal Justice No. 408', Australian Institute of Criminology, Australia.

Choo, K.K.R. (2011b). 'The cyber threat landscape: challenges and future research directions', *Computers & Security*, 30*(8)*, pp. 719-731.

Choo, K.K.R. (2008). 'Organised crime groups in cyberspace: a typology', *Trends in Organized Crime*, 11*(3)*, pp. 270-295.

Choo, K.K.R. & Smith, R.G. (2008). 'Criminal exploitation of online systems by organised crime groups', *Asian Journal of Criminology*, 3*(1)*, pp. 37-59.

Chuang, J., Nguyen, H., Wang, C. & Johnson, B. (2013). 'I think, therefore I am: usability and security of authentication using brainwaves', *International Conference on Financial Cryptography and Data Security*, Springer, Okinawa, Japan, 1-5 April, pp. 1-16.

Clough, J. (2010). *Principles of Cybercrime*, Cambridge University Press, Cambridge.

Comer, R., McKelvey, N. & Curran, K. (2012). 'Privacy and Facebook', *International Journal of Engineering and Technology*, 2*(9)*, pp. 1626-1630.

Comrey, A.L. & Lee, H.B. (1992). *A First Course in Factor Analysis*, 2nd ed., Psychology Press, New York, NY.

Cranor, L. & Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly Media, Sebastopol, CA.

Creswell, J.W. (2010). ‘Mapping the developing landscape of mixed methods research’, In: A. Tashakkori & C. Teddlie (eds.), *SAGE Handbook of Mixed Methods in Social & Behavioral Research*, 2nd ed., pp. 45-68, Sage Publications, Thousand Oaks, CA.

Creswell, J.W. & Clark, V.L.P. (2017). *Designing and Conducting Mixed Methods Research*, 3rd ed., Sage Publications, Thousand Oaks, CA.

Creswell, J.W. & Creswell, J.D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed., Sage Publications, Thousand Oaks, CA.

Creswell, J.W. & Poth, C.N. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th ed., Sage Publications, Thousand Oaks, CA.

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., Thomas, L. & Barnes, A. (2016). ‘Longitudinal impact of the cyber-friendly schools program on adolescents’ cyberbullying behaviour’, *Aggressive Behaviour*, 42*(2)*, pp. 166-180.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). ‘Future directions for behavioral information security research’, *Computers & Security*, 32*(2013)*, pp. 90-101.

Cybercrime Bill (2017). *Cybercrimes and Cybersecurity Bill 2017*, available from: http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf, Department of Justice, Pretoria, [last accessed: 25 January 2018].

Deng, L., Turner, D.E., Gehling, R. & Prince, B. (2010). ‘User experience, satisfaction, and continual usage intention of IT’, *European Journal of Information Systems*, 19*(1)*, pp. 60-75.

Denning, P.J. & Denning, D.E. (2010). ‘Discussing cyberattack’, *Communications of the ACM*, 53*(9)*, pp. 29-31.

Denzin, N.K. (2012). ‘Triangulation 2.0.’, *Journal of Mixed Methods Research*, 6*(2)*, pp. 80-88.

Denzin, N.K. & Lincoln, Y.S. (eds.) (2017). *The SAGE Handbook of Qualitative Research*, 5th ed., Sage Publications, Thousand Oaks, CA.

Denzin, N.K. & Lincoln, Y.S. (eds.) (2013). *The Landscape of Qualitative Research*, 4th ed., Sage Publications, Thousand Oaks, CA.

Desurvire, H. & Wiberg, C. (2015). ‘User experience design for inexperienced gamers: GAP – Game Approachability Principles’, In: R. Bernhaupt (ed.), *Game User Experience Evaluation: Concepts and Methods*, pp. 169-186, Springer International Publishing, Sebastopol, CA.

Dhami, A., Agarwal, N., Chakraborty, T.K., Singh, B.P. & Minj, J. (2013). ‘Impact of trust, security and privacy concerns in social networking: an exploratory study to understand the pattern of information revelation in Facebook’, *Proceedings of the 3rd IEEE International Advance Computing Conference (IACC)*, IEEE, Ghaziabad, 22-23 February, pp. 465-469.

Dhamija, R. & Perrig, A. (2000). ‘Deja vu: a user study using images for authentication’, *Proceedings of the 9th Conference on USENIX Security Symposium Volume 9*, USENIX Association, Denver, CO, 14-17 August, pp. 1-14.

Dhamija, R., Tygar, J.D. & Hearst, M. (2006). ‘Why phishing works’, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Montréal, 22-27 April, pp. 581-590.

Dodds, W.B., Monroe, K.B. & Grewal, D. (1991). ‘Effects of price, brand, and store information on buyers’ product evaluations’, *Journal of Marketing Research*, 28*(3)*, pp. 307-319.

Dourish, P., Grinter, R.E., De la Flor, J.D. & Joseph, M. (2004). ‘Security in the wild: user strategies for managing security as an everyday, practical problem’, *Personal and Ubiquitous Computing*, 8*(6)*, pp. 391-401.

Dourish, P. & Redmiles, D. (2002). ‘An approach to usable security based on event monitoring and visualization’, *Proceedings of the 2002 Workshop on New Security Paradigms*, ACM, Virginia Beach, VA, 23-26 September, pp. 75-81.

Downs, J.S., Holbrook, M.B. & Cranor, L.F. (2007). ‘Behavioral response to phishing risk’, *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, ACM, Pittsburgh, PA, 4-5 October, pp. 37-44.

Downs, J.S., Holbrook, M.B. & Cranor, L.F. (2006). ‘Decision strategies and susceptibility to phishing’, *Proceedings of the 2nd Symposium on Usable Privacy and Security*, ACM, Pittsburgh, PA, 12-14 July, pp. 79-90.

Doyle, L., Brady, A. & Byrne, G. (2009). ‘An overview of mixed methods research’, *Journal of Research in Nursing*, 14*(2)*, pp. 175-185.

Edwards, C. (2014). ‘Ending identity theft and cybercrime’, *Biometric Technology Today*, 2014*(2)*, pp. 9-11.

Endsley, M.R. & Jones, D.G. (2011). *Designing for Situation Awareness: An Approach to User-Centered Design*, 2nd ed., CRC Press, Boca Raton, FL.

Erasmus, J. (2015). *Identity theft in SA booming*, available from: http://www.news24.com/SouthAfrica/News/Identity-theft-in-SA-booming-20150522, News24, South Africa, [last accessed: 25 January 2018].

Fiegerman, S. (2017). *Marissa Mayer grilled by Congress over massive Yahoo security breach*, available from: http://money.cnn.com/2017/11/08/technology/marissa-mayer-congress/index.html, CNN Money, Atlanta, GA, [last accessed: 25 January 2018].

FinMark Trust (2016). *FinScope South Africa 2016*, available from: http://www.finmark.org.za/wp-content/uploads/2017/12/08Nov2016_FinScope_Consumer-survey-South-Africa-2016.pdf, FinMark Trust, Johannesburg, [last accessed: 25 January 2018].

Flechais, I., Mascolo, C. & Sasse, M.A. (2007). 'Integrating security and usability into the requirements and design process', *International Journal of Electronic Security and Digital Forensics*, 1*(1)*, pp. 12-26.

Fleetwood, S. & Ackroyd, S. (2004). *Critical Realist Applications in Organisation and Management Studies*, Routledge, London.

Forsythe, S.M. & Shi, B. (2003). 'Consumer patronage and risk perceptions in internet shopping', *Journal of Business Research*, 56*(11)*, pp. 867-875.

Fraser, A. (2017). *Revealed: the real source of SA's massive data breach*, available from: https://techcentral.co.za/revealed-real-source-sas-massive-data-breach/77626/, TechCentral, Johannesburg, [last accessed: 25 January 2018].

Gale, N.K., Heath, G., Cameron, E., Rashid, S. & Redwood, S. (2013). 'Using the framework method for the analysis of qualitative data in multi-disciplinary health research', *BMC Medical Research Methodology*, 13*(1)*, pp. 117-124.

Garfinkel, S. & Lipford, H.R. (2014). 'Usable security: history, themes, and challenges', *Synthesis Lectures on Information Security, Privacy, and Trust*, 5*(2)*, pp. 1-124.

Georgsson, M. & Staggers, N. (2016). 'An evaluation of patients' experienced usability of a diabetes mHealth system using a multi-method approach', *Journal of Biomedical Informatics*, 59*(2016)*, pp. 115-129.

Gibbs, G.R. (2007). *Analyzing Qualitative Data*, Sage Publications, London.

Given, L.M. (ed.) (2008). *The SAGE Encyclopedia of Qualitative Research Methods*, Sage Publications, Thousand Oaks, CA.

Gkoutzinis, A.A. (2006). *Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce*, Cambridge University Press, London.

Glasser, D. & Taneja, A. (2015). 'A routine activity theory-based framework for combating cybercrime', In: M.M. Cruz-Cunha & I.M. Portela (eds.), *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, pp. 398-406, IGI Global, Hershey, PA.

Gollmann, D. (2011). *Computer Security*, 3rd ed., Wiley, Chichester.

Gonzalez-Garcia, J. (2017). *Online and mobile banking statistics*, available from: http://www.creditcards.com/credit-card-news/online-mobile-banking.php, Creditcards.com, Austin, TX, [last accessed: 25 January 2018].

Gould, J.D. & Lewis, C. (1985). 'Designing for usability: key principles and what designers think', *Communications of the ACM*, 28*(3)*, pp. 300-311.

Grabosky, P. (2014). 'The global dimension of cybercrime', In: M. Galeotti (ed.), *Global Crime Today: The Changing Face of Organised Crime* Routledge, New York, NY.

Graham, J., Olson, R. & Howard, R. (eds.) (2011). *Cyber Security Essentials*, CRC Press, Boka Raton, FL.

Graham, L. (2017). *Cybercrime costs the global economy $450 billion: CEO*, available from: https://finance.yahoo.com/news/cybercrime-costs-global-economy-450-150048096.html, Yahoo Finance, Sunnyvale, CA, [last accessed: 25 January 2018].

Gray, D.E. (2014). *Doing Research in the Real World*, 3rd ed., Sage Publications, London.

Green, M. & Smith, M. (2016). 'Developers are not the enemy!: the need for usable security APIs', *IEEE Security & Privacy*, 14*(5)*, pp. 40-46.

Greene, J.C., Caracelli, V.J. & Graham, W.F. (1989). 'Toward a conceptual framework for mixed-method evaluation designs', *Educational Evaluation and Policy Analysis*, 11*(3)*, pp. 255-274.

Greene, J.C. & Hall, J.N. (2010). 'Dialectics and pragmatism: being of consequence', In: A. Tashakkori & C. Teddlie (eds.), *SAGE Handbook of Mixed Methods in Social & Behavioral Research*, 2nd ed., pp. 45-68, Sage Publications, Thousand Oaks, CA.

Grudin, J. (2012). 'A moving target: the evolution of HCI', In: A. Sear & J.A. Jacko (eds.), *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, 3rd ed., pp. xxvii-Ixi, Lawrence Erlbaum Associates, Boca Raton, FL.

Haase, A. (2015). 'Harmonizing substantive cybercrime law through European Union directive 2013/40/EU: from European legislation to international model law?', *Proceedings of the First International Conference on Anti-Cybercrime (ICACC)*, IEEE, Riyadh, 10-12 November, pp. 1-6.

Hadid, A., Evans, N., Marcel, S. & Fierrez, J. (2015). 'Biometrics systems under spoofing attack: an evaluation methodology and lessons learned', *IEEE Signal Processing Magazine*, 32*(5)*, pp. 20-30.

Hair Jr., J.F., Black, W.C., Babin, B.J. & Anderson, R.E. (2014). *Multivariate Data Analysis*, 7th ed., Pearson Education, Essex.

Hair Jr., J.F., Hult, G.T.M., Ringle, C. & Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd ed., Sage Publications, London.

Han, K.S. & Noh, M.H. (1999). 'Critical failure factors that discourage the growth of electronic commerce', *International Journal of Electronic Commerce*, 4*(2)*, pp. 25-43.

Harrell, E. (2015). 'Victims of Identity Theft, 2014', U.S. Department of Justice, Washington, D.C.

Hassenzahl, M., Platz, A., Burmester, M. & Lehner, K. (2000). 'Hedonic and ergonomic quality aspects determine a software's appeal', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, The Hague, 1-6 April, pp. 201-208.

He, D., Chan, S. & Guizani, M. (2015). 'Mobile application security: malware threats and defenses', *IEEE Wireless Communications*, 22*(1)*, pp. 138-144.

Hernando, I. & Nieto, M.J. (2007). 'Is the internet delivery channel changing banks' performance? The case of Spanish banks', *Journal of Banking & Finance*, 31*(4)*, pp. 1083-1099.

Hertzum, M., Molich, R. & Jacobsen, N.E. (2014). 'What you get is what you see: revisiting the evaluator effect in usability tests', *Behaviour & Information Technology*, 33*(2)*, pp. 144-162.

Hille, P., Walsh, G. & Cleveland, M. (2015). 'Consumer fear of online identity theft: scale development and validation', *Journal of Interactive Marketing*, 30*(2015)*, pp. 1-19.

Ho, A.T. (2006). 'Accounting for the value of performance measurement from the perspective of Midwestern mayors', *Journal of Public Administration Research and Theory*, 16*(2)*, pp. 217-237.

Hof, H.-. (2013). 'Towards enhanced usability of IT security mechanisms – how to design usable IT security mechanisms using the example of email encryption', *International Journal on Advances in Security*, 6*(1)*, pp. 78-87.

Hong, J. (2012). 'The state of phishing attacks', *Communications of the ACM*, 55*(1)*, pp. 74-81.

Hornbæk, K. (2006). 'Current practice in measuring usability: challenges to usability studies and research', *International Journal of Human-Computer Studies*, 64*(2)*, pp. 79-102.

Hu, Q., Dinev, T., Hart, P. & Cooke, D. (2012). 'Managing employee compliance with information security policies: the critical role of top management and organizational culture', *Decision Sciences*, 43*(4)*, pp. 615-660.

Hyman, P. (2013). 'Cybercrime: it's serious, but exactly how serious?', *Communications of the ACM*, 56*(3)*, pp. 18-20.

IEA (2018). *Definition and domains of ergonomics*, available from: http://www.iea.cc/whats/index.html, IEA, Zurich, [last accessed: 25 January 2018].

IEEE Std. 610.12 (1990). 'IEEE standard glossary of software engineering terminology', IEEE, New York, NY.

Iivari, J. & Hirschheim, R. (1996). 'Analyzing information systems development: a comparison and analysis of eight IS development approaches', *Information Systems*, 21*(7)*, pp. 551-575.

Information is Beautiful (2018). *World's biggest data breaches*, available from: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, Information is Beautiful, London, [last accessed: 25 January 2018].

Internet Live Stats (2018). *South Africa internet users*, available from: http://www.internetlivestats.com/internet-users/south-africa/, Internet Live Stats, [last accessed: 25 January 2018].

IOL (2016). *Cybercrime: 8.8m South Africans victim in 2015*, available from: https://www.iol.co.za/business-report/economy/cybercrime-88m-safricans-victim-in-2015-2041922, IOL, Johannesburg, [last accessed: 25 January 2018].

Ismail, A. (2017). *SIM-swap victims mull legal action against banks*, available from: http://www.fin24.com/Companies/Financial-Services/sim-swap-victims-mull-legal-action-against-banks-20170424, News24, Johannesburg, [last accessed: 25 January 2018].

ISO 9241-11 (1998). 'Ergonomic requirements for office work with visual display terminals (VDTs): guidance on usability', International Standards Organisation, Geneva.

ISO 9241-210 (2010). 'Ergonomics of human system interaction – part 210: human-centered design for interactive systems', International Standards Organisation, Geneva.

ISO/IEC 25010 (2011). 'Systems and software engineering–systems and software quality requirements and evaluation (SQuaRE) – system and software quality models', International Standards Organisation, Geneva.

ISO/IEC 9126-1 (2001). 'Software engineering – product quality – part 1: quality model', International Standards Organisation, Geneva.

ISO/IEC 9126-4 (2004). 'Software engineering – product quality – part 4: quality in use metrics', International Standards Organisation, Geneva.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. & Menczer, F. (2007). 'Social phishing', *Communications of the ACM*, 50*(10)*, pp. 94-100.

Johnson, J. (2013). *Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Guidelines*, 2nd ed., Elsevier, Waltham, MA.

Johnson, R.B. & Gray, R. (2010). 'A history of philosophical and theoretical issues for mixed methods research', In: A. Tashakkori & C. Teddlie (eds.), *SAGE Handbook of Mixed Methods in Social and Behavioral Research*, 2nd ed., pp. 69-94, Sage Publications, Thousand Oaks, CA.

Johnson, R.B. & Onwuegbuzie, A.J. (2004). 'Mixed methods research: a research paradigm whose time has come', *Educational Researcher*, 33*(7)*, pp. 14-26.

Johnson, R.B., Onwuegbuzie, A.J. & Turner, L.A. (2007). 'Toward a definition of mixed methods research', *Journal of Mixed Methods Research*, 1*(2)*, pp. 112-133.

Johnston, J., Eloff, J.H.P. & Labuschagne, L. (2003). 'Security and human computer interfaces', *Computers & Security*, 22*(8)*, pp. 675-684.

Kaplan, B. & Duchon, D. (1988). 'Combining qualitative and quantitative methods in information systems research: a case study', *MIS Quarterly*, 12*(4)*, pp. 571-586.

Karat, C.M., Brodie, C. & Karat, J. (2005). 'Usability design and evaluation for privacy and security solutions', In: L.F. Cranor & S. Garfinkel (eds.), *Security and Usability: Designing Secure Systems That People Can Use*, pp. 47-74, O'Reilly Media, Sebastopol, CA.

Kaspersky Lab & B2B International (2016). 'Consumer security risks survey 2016: connected but not protected', Kaspersky Lab and B2B International, London.

Kaspersky Lab & B2B International (2014). ‘Consumer security risks survey 2014: multi-device threats in a multi-device world’, Kaspersky Lab and B2B International, London.

Katsabas, D., Furnell, S. & Dowland, P. (2005). ‘Using human computer interaction principles to promote usable security’, *Proceedings of the 5th International Network Conference*, NRG, Samos, Greece, 5-7 July, pp. 235-242.

Kitchenham, B. & Pfleeger, S.L. (2002). ‘Principles of survey research: part 5: populations and samples’, *ACM SIGSOFT Software Engineering Notes*, 27*(5)*, pp. 17-20.

Kline, R.B. (2015). *Principles and Practice of Structural Equation Modeling*, 4th ed., Guilford Publications, New York, NY.

Kraemer, S., Carayon, P. & Clem, J. (2009). ‘Human and organizational factors in computer and information security: pathways to vulnerabilities’, *Computers & Security*, 28*(7)*, pp. 509-520.

Krol, K., Philippou, E., De Cristofaro, E. & Sasse, M.A. (2015). ‘“They brought in the horrible key ring thing!” Analysing the usability of two-factor authentication in UK online banking’, *USEC 2015: NDSS Workshop on Usable Security*, Internet Society, San Diego, CA, 8 February, pp. 1-10.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2015). ‘Advanced social engineering attacks’, *Journal of Information Security and Applications*, 22*(2015)*, pp. 113-122.

Law, E.L., Roto, V., Hassenzahl, M., Vermeeren, A.P.O.S. & Kort, J. (2009). ‘Understanding, scoping and defining user experience: a survey approach’, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Boston, MA, 7 April, pp. 719-728.

Lazar, J., Feng, J.H. & Hochheiser, H. (2010). *Research Methods in Human-Computer Interaction*, John Wiley & Sons, Glasgow.

Lehto, M.R. & Landry, S.J. (2012). *Introduction to Human Factors and Ergonomics for Engineers*, 2nd ed., CRC Press, Boca Raton, FL.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolff, S. (2009). ‘A brief history of the internet’, *ACM SIGCOMM Computer Communication Review*, 39*(5)*, pp. 22-31.

Levin, M. & Greenwood, D. (2013). ‘Revitalizing universities by reinventing the social sciences’, In: N.K. Denzin & Y.S. Lincoln (eds.), *The Landscape of Qualitative Research*, 4th ed., pp. 55-87, Sage Publications, Thousand Oaks, CA.

Limayem, M., Hirt, S.G. & Cheung, C.M.K. (2007). ‘How habit limits the predictive power of intention: the case of information systems continuance’, *MIS Quarterly*, 31*(4)*, pp. 705-737.

Lincoln, Y.S. & Guba, E.G. (1985). *Naturalistic Inquiry*, Sage Publications, Newbury Park, CA.

Lincoln, Y.S., Lynham, S.A. & Guba, E.G. (2013). ‘Paradigmatic controversies, contradictions, and emerging confluences, revisited’, In: N.K. Denzin & Y.S. Lincoln (eds.), *The Landscape of Qualitative Research*, 4th ed., pp. 199-265, Sage Publications, Inc., Thousand Oaks, CA.

Littler, D. & Melanthiou, D. (2006). ‘Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: the case of internet banking’, *Journal of Retailing and Consumer Services*, 13*(6)*, pp. 431-443.

Liu, Y., Goncalves, J., Ferreira, D., Xiao, Hosio, S. & Kostakos, V. (2014). ‘CHI 1994-2013: mapping two decades of intellectual progress through co-word analysis’, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Toronto, Canada, 26 April - 1 May, pp. 3553-3562.

Loader, B.D. & Thomas, D. (eds.) (2013). *Cybercrime: Security and Surveillance in the Information Age*, Routledge, London.

Matyas, V. & Riha, Z. (2002). ‘Biometric authentication – security and usability’, *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, Kluwer Academic Pub, Portorož, 26-27 September, pp. 227-239.

Maughan, D. (2009). ‘A Roadmap for Cybersecurity Research’, US Department of Homeland Security, Washington D.C., USA.

McDaniel, G. (1994). *IBM Dictionary of Computing*, McGraw-Hill, New York, NY.

McLellan, S., Muddimer, A. & Peres, S.C. (2012). ‘The effect of experience on system usability scale ratings’, *Journal of Usability Studies*, 7*(2)*, pp. 56-67.

Mertens, D.M. (2007). ‘Transformative paradigm: mixed methods and social justice’, *Journal of Mixed Methods Research*, 1*(3)*, pp. 212-225.

Mi, N., Cavuoto, L.A., Benson, K., Smith-Jackson, T. & Nussbaum, M.A. (2014). ‘A heuristic checklist for an accessible smartphone interface design’, *Universal Access in the Information Society*, 13*(4)*, pp. 351-365.

Mingers, J. (2001). ‘Combining IS research methods: towards a pluralist methodology’, *Information Systems Research*, 12*(3)*, pp. 240-259.

Mitnick, K.D. & Simon, W.L. (2005). *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders and Deceivers*, Wiley Publishing, Indianapolis, IN.

Mitnick, K.D. & Simon, W.L. (2002). *The Art of Deception: Controlling the Human Element of Security*, Wiley Publishing, Indianapolis, IN.

Montazemi, A.R. & Qahri-Saremi, H. (2015). ‘Factors affecting adoption of online banking: a meta-analytic structural equation modeling study’, *Information & Management*, 52*(2)*, pp. 210-226.

Morgan, D.L. (2014). *Integrating Qualitative and Quantitative Methods: A Pragmatic Approach*, Sage Publications, Thousand Oaks, CA.

Morgan, S. (2016). *Cybercrime costs projected to reach $2 trillion by 2019*, available from: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3b8369783a91, Forbes, New York, NY, [last accessed: 25 January 2018].

Morosan, C. (2012). 'Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: extending the technology acceptance model', *Journal of Hospitality & Tourism Research*, 36*(1)*, pp. 52-84.

Morse, J.M. (2010). 'Principles of mixed methods and multimethod research design', In: A. Tashakkori & C. Teddlie (eds.), *SAGE Handbook of Mixed Methods in Social and Behavioral Research*, 2nd ed., pp. 189-208, Sage Publications, Thousand Oak, CA.

Mouton, F., Malan, M.M., Kimppa, K.K. & Venter, H.S. (2015). 'Necessity for ethics in social engineering research', *Computers & Security*, 55*(2015)*, pp. 114-127.

Mujinga, M., Eloff, M.M. & Kroeze, J.H. (2016). 'Online banking users' perceptions in South Africa: an exploratory empirical study', *Proceedings of IST-Africa 2016 Conference*, IIMC, Durban, South Africa, 11-13 May, pp. 1-7.

Myers, M.D. (2013). *Qualitative Research in Business and Management*, 2nd ed., Sage Publications, London.

Nardi, P.M. (2014). *Doing Survey Research*, 3rd ed., Paradigm Publishers, Boulder, CO.

Newman, L.H. (2017). *Equifax officially has no excuse*, available from: https://www.wired.com/story/equifax-breach-no-excuse/, Wired, San Francisco, CA, [last accessed: 25 January 2018].

Nielsen, J. (2010). 'What is usability?', In: C. Wilson (ed.), *User Experience Re-Mastered: Your Guide to Getting the Right Design*, pp. 3-22, Morgan Kaufmann, Burlington, MA.

Nielsen, J. (2000). *Designing Web Usability: The Practice of Simplicity*, New Riders Publishing, Berkeley, CA.

Nielsen, J. (1995). *Ten usability heuristics*, available from: http://www.nngroup.com/articles/ten-usability-heuristics/, Nielsen Norman Group, Fremont, CA, [last accessed: 25 January 2018].

Nielsen, J. (1994a). 'Enhancing the explanatory power of usability heuristics', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Boston, MA, 24-28 April, pp. 152-158.

Nielsen, J. (1994b). 'Heuristic evaluation', In: J. Nielsen & R.L. Mack (eds.), *Usability Inspection Methods*, pp. 25-62, John Wiley & Sons, New York, NY.

Nielsen, J. (1994c). 'Usability inspection methods', *Conference Companion on Human Factors in Computing Systems*, ACM, Boston, MA, 24-28 April, pp. 413-414.

O'Brien, H.L. (2010). 'The influence of hedonic and utilitarian motivations on user engagement: the case of online shopping experiences', *Interacting with Computers*, 22*(5)*, pp. 344-352.

O'Rourke, N. & Hatcher, L. (2013). *A Step-by-Step Approach to Using SAS for Factor Analysis and Structural Equation Modeling*, 2nd ed., SAS Institute, Cary, NC.

Oates, B.J. (2006). *Researching Information Systems and Computing*, Sage Publications, London.

Ogara, S.O., Koh, C.E. & Prybutok, V.R. (2014). 'Investigating factors affecting social presence and user satisfaction with mobile instant messaging', *Computers in Human Behavior*, 36*(2014)*, pp. 453-459.

Oppliger, R. (1997). 'Internet security: firewalls and beyond', *Communications of the ACM*, 40*(5)*, pp. 92-102.

Oxford Dictionary (2018). *Oxford English Dictionary Online*, available from: http://www.oxforddictionaries.com, Oxford University Press, Oxford, [last accessed: 25 January 2018].

Pallant, J. (2013). *SPSS Survival Manual*, 5th ed., McGraw-Hill Education, Berkshire.

Parker, D.B. (2012). 'Toward a new framework for information security?', In: S. Bosworth, M.E. Kabay & E. Whyne (eds.), *Computer Security Handbook*, 6th ed., pp. 3.1-3.23, John Wiley & Sons, Hoboken, NJ.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). 'Human factors and information security: individual, culture and security environment', DTIC Document, Edinburgh.

Patel, V.M., Chellappa, R., Chandra, D. & Barbello, B. (2016). 'Continuous user authentication on mobile devices: recent progress and remaining challenges', *IEEE Signal Processing Magazine*, 33*(4)*, pp. 49-61.

Payne, S.C., Youngcourt, S.S. & Beaubien, J.M. (2007). 'A meta-analytic examination of the goal orientation nomological net', *Journal of Applied Psychology*, 92*(1)*, pp. 128.

Payne, S.J. (2012). 'Human models in human-computer interaction', In: A. Sears & J.A. Jacko (eds.), *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, 3rd ed., pp. 41-54, CRC Press, New York, NY.

Peltier, T.R. (2014). *Information Security Fundamentals*, 2nd ed., CRC Press, Boca Raton, FL.

Peltier, T.R., Peltier, J. & Blackley, J. (2005). *Information Security Fundamentals*, CRC Press, Boca Raton, FL.

Perlroth, N. (2017). *All 3 billion Yahoo accounts were affected by 2013 attack*, available from: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html, NY Times, New York, NY, [last accessed: 25 January 2018].

Petrie, H. & Bevan, N. (2009). 'The evaluation of accessibility, usability and user experience', In: C. Stepanidis (ed.), *The Universal Access Handbook*, pp. 20-1-20-30, CRC Press, Boca Raton, FL.

Pfleeger, C.P. & Pfleeger, S.L. (2015). *Security in Computing*, 5th ed., Prentice Hall, Boston, MA.

Pipkin, D.L. (2000). *Information Security: Protecting the Global Enterprise*, Prentice Hall, Upper Saddle River, NJ.

Plateaux, A., Lacharme, P., Jøsang, A. & Rosenberger, C. (2014). 'One-time biometrics for online banking and electronic payment authentication', *International Conference on Availability, Reliability, and Security*, Springer, Fribourg, 8-12 September, pp. 179-193.

Pons, A.P. & Polak, P. (2008). 'Understanding user perspectives on biometric technology', *Communications of the ACM*, 51*(9)*, pp. 115-118.

Poon, W. (2008). 'Users' adoption of e-banking services: the Malaysian perspective', *Journal of Business & Industrial Marketing*, 23*(1)*, pp. 59-69.

PoPI (2013). *Protection of Personal Information Act (POPI) 4 of 2013*, available from: https://www.justice.gov.za/legislation/acts/2013-004.pdf, Department of Justice, Pretoria, [last accessed: 25 January 2018].

Preece, J., Rogers, Y. & Sharp, H. (2015). *Interaction Design: Beyond Human-Computer Interaction*, 4th ed., John Wiley & Sons, Chichester.

Prettyman, S.S., Furman, S., Theofanos, M. & Stanton, B. (2015). 'Privacy and security in the brave new world: the use of multiple mental models', In: T. Tryfonas & I. Askoxylakis (eds.), *Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science, vol 9190*, pp. 260-270, Springer.

Proctor, R.W. & Vu, K.P.L. (2012). 'Human information processing: an overview for human-computer interaction', In: A. Sears & J.A. Jacko (eds.), *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, 3rd ed., pp. 21-40, CRC Press, New York, NY.

Rege, A. (2016). 'Incorporating the human element in anticipatory and dynamic cyber defense', *Proceedings of the IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, IEEE, Vancouver, 12-14 June, pp. 1-7.

Rencher, A.C. & Christensen, W.F. (2012). *Methods of Multivariate Analysis*, 3rd ed., John Wiley & Sons, New York, NY.

Ritchie, J. & Spencer, L. (2002). 'Qualitative data analysis for applied policy research', In: A.M. Huberman & M.B. Miles (eds.), *The Qualitative Researcher's Companion*, pp. 305-329, Sage Publications, Thousand Oaks, CA.

Ropohl, G. (1999). 'Philosophy of socio-technical systems', *Techné: Research in Philosophy and Technology*, 4*(3)*, pp. 186-194.

RSA (2015). ‘2014 cybercrime roundup: the year of the POS breach’, RSA, Bedford, MA.

RSA (2014). ‘Phishing kits – the same wolf, just a different sheep’s clothing’, RSA, Bedford, MA.

Rubin, J. & Chisnell, D. (2008). *Handbook of Usability Testing: How to Plan, Design and Conduct Effective Tests*, 2nd ed., John Wiley & Sons, Indianapolis, IN.

SABRIC (2018). *South African Banking Risk Information Centre (SABRIC)*, available from: https://www.sabric.co.za/about-us, SABRIC, Johannesburg, [last accessed: 25 January 2018].

SABRIC (2017). *Release of card fraud stats 2016*, available from: https://www.sabric.co.za/media-and-news/posts/release-of-card-fraud-stats-2016/, SABRIC, Johannesburg, [last accessed: 25 January 2018].

Saldaña, J. (2016). *The Coding Manual for Qualitative Researchers*, 3rd ed., Sage Publications, London.

Saltzer, J.H. & Schroeder, M.D. (1975). ‘The protection of information in computer systems’, *Proceedings of the IEEE*, 63*(9)*, pp. 1278-1308.

Saridakis, G., Benson, V., Ezingeard, J. & Tennakoon, H. (2015). ‘Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users’, *Technological Forecasting and Social Change*, 102*(2015)*, pp. 320-330.

Sasse, M.A. & Flechais, I. (2005). ‘Usable security: why do we need it? How do we get it?’, In: L.F. Cranor & S. Garfinkel (eds.), *Security and Usability: Designing Secure Systems That People Can Use*, pp. 13-30, O’Reilly Media, Sebastopol, CA.

Saunders, K.M. & Zucker, B. (1999). ‘Counteracting identity fraud in the information age: the identity theft and assumption deterrence act’, *International Review of Law, Computers & Technology*, 13*(2)*, pp. 183-192.

Saunders, M., Lewis, P. & Thornhill, A. (2016). *Research Methods for Business Students*, 7th ed., Pearson Education, Essex, England.

Sawyer, B.D., Finomore, V.S., Funke, G.J., Mancuso, V.F., Miller, B., Warm, J. & Hancock, P.A. (2015). ‘Evaluating cybersecurity vulnerabilities with the email testbed: effects of training’, *Proceedings 19th Triennial Congress of the IEA*, IEA, Melbourne, 9-14 August, pp. 14-19.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, New York, NY.

Schutt, R.K. (2015). *Investigating the Social World: The Process and Practice of Research*, 8th ed., Sage Publications, Thousand Oaks, CA.

Selim, H.M. (2003). ‘An empirical investigation of student acceptance of course websites’, *Computers & Education*, 40*(4)*, pp. 343-360.

Selim, H.M. (2005). ‘Video conferencing-mediated instruction: success model’, *International Journal of Distance Education Technologies (IJDET)*, 3*(1)*, pp. 62-80.

Shah, M.H. & Siddiqui, F.A. (2006). 'Organisational critical success factors in adoption of e-banking at the Woolwich bank', *International Journal of Information Management*, 26*(6)*, pp. 442-456.

Shaikh, A.A. & Karjaluoto, H. (2015). 'Mobile banking adoption: A literature review', *Telematics and Informatics*, 32*(1)*, pp. 129-142.

Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. & Cranor, L.F. (2014). 'Can long passwords be secure and usable?', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Toronto, Canada, 26 April-1 May, pp. 2927-2936.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J. (2010). 'Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Atlanta, GA, 10-15 April, pp. 373-382.

Shiferaw, F. & Zolfo, M. (2012). 'The role of information communication technology (ICT) towards universal health coverage: the first steps of a telemedicine project in Ethiopia', *Global Health Action*, 5*(1)*, pp. 1-8.

Shirey, R. (2000). 'RFC 2828: Internet Security Glossary', Internet Engineering Task Force.

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N. & Diakopoulos, N. (2016). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*, 6th ed., Pearson Education, Hoboken, NJ.

Sikdar, P., Kumar, A. & Makkad, M. (2015). 'Online banking adoption: A factor validation and satisfaction causation study in the context of Indian banking customers', *International Journal of Bank Marketing*, 33*(6)*, pp. 760-785.

Silverman, D. (2014). *Interpreting Qualitative Data*, 5th ed., Sage Publications, London.

Srivastava, A. & Thomson, S.B. (2009). 'Framework analysis: a qualitative methodology for applied policy research', *Journal of Administration and Governance*, 4*(2)*, pp. 72-79.

Stallings, W. (2011a). *Cryptography and Network Security: Principles and Practice*, 5th ed., Prentice Hall, Upper Saddle River, NJ.

Stallings, W. (2011b). *Network Security Essentials: Applications and Standards*, 4th ed., Prentice Hall, Upper Saddle River, NJ.

Stamp, M. (2011). *Information Security: Principles and Practice*, 2nd ed., John Wiley & Sons, Hoboken, NJ.

Stanton, J.M. & Stam, K.R. (2006). *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets -- Without Compromising Employee Privacy or Trust*, Information Today, Medford, NJ.

Statista (2015). *Online banking penetration in selected European markets in 2014*, available from: https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/, Statista, New York, NY, [last accessed: 25 January 2018].

Statista (2012). *Global online banking penetration in April 2012, by region*, available from: https://www.statista.com/statistics/233284/development-of-global-online-banking-penetration/, Statista, New York, NY, [last accessed: 25 January 2018].

Stats SA (2016). 'Mid-Year Population Estimates 2015', Stats SA, Pretoria.

Symantec (2015). 'Internet Security Threat Report, Volume 20 2015', Symantec, Mountain View, CA.

Tabachnick, B.G. & Fidell, L.S. (2014). *Using Multivariate Statistics*, 6th ed., Pearson Education, Essex.

Talabis, M. & Martin, J. (2013). *Information Security Risk Assessments Toolkit*, Elsevier, Waltham, MA.

Tarhini, A., Mgbemena, C., Trab, M.S.A. & Masa'Deh, R. (2015). 'User adoption of online banking in Nigeria: a qualitative study', *The Journal of Internet Banking and Commerce*, 20*(3)*, pp. 1-16.

Tashakkori, A. & Teddlie, C. (2010). *SAGE Handbook of Mixed Methods in Social and Behavioral Research*, 2nd ed., Sage Publications, Thousand Oaks, CA.

Theofanos, M.F. & Pfleeger, S.L. (2011). 'Guest editors' introduction: shouldn't all security be usable?', *IEEE Security and Privacy*, 9*(2011)*, pp. 12-17.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). 'The insider threat to information systems and the effectiveness of ISO17799', *Computers & Security*, 24*(6)*, pp. 472-484.

Thomson, K.L. & Von Solms, R. (2005). 'Information security obedience: a definition', *Computers & Security*, 24*(1)*, pp. 69-75.

Touhill, G.J. & Touhill, C.J. (2014). *Cybersecurity for Executives: A Practical Guide*, John Wiley & Sons, Hoboken, NJ.

Tryfonas, T. (2010). 'Information security management and standards of best practice', In: H. Jahankhani, D.L. Watson, G. Me & F. Leonhardt (eds.), *Handbook of Electronic Security and Digital Forensics*, pp. 207-236, World Scientific Publishing Co., Singapore.

Turban, E., King, D., Lee, J.K., Liang, T. & Turban, D.C. (2015). *Electronic Commerce: A Managerial and Social Networks Perspective*, Springer, London.

Van Gemert-Pijnen, J.E., Nijland, N., Van Limburg, M., Ossebaard, H.C., Kelders, S.M., Eysenbach, G. & Seydel, E.R. (2011). 'A holistic framework to improve the uptake and impact of ehealth technologies', *Journal of Medical Internet Research*, 13*(4)*, pp. e111.

Van Hamme, T., Rimmer, V., Preuveneers, D., Joosen, W., Mustafa, M.A., Abidin, A. & Rúa, E.A. (2017). 'Frictionless authentication systems: emerging trends, research challenges and opportunities', *Proceedings of the 11th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2017)*, IARIA, Rome, Italy, 10-14 September, pp. 1-5.

Van Zyl, G. (2015). *FNB rated SA's 'top internet banking provider'*, available from: http://www.fin24.com/Tech/News/FNB-rated-SAs-top-internet-banking-provider-20150507, Fin24, Johannesburg, [last accessed: 25 January 2018].

Vasiete, E., Chen, Y., Char, I., Yeh, T., Patel, V., Davis, L. & Chellappa, R. (2014). 'Toward a non-intrusive, physio-behavioral biometric for smartphones', *Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services*, ACM, Toronto, 23-26 September, pp. 501-506.

Vatanasombut, B., Igbaria, M., Stylianou, A.C. & Rodgers, W. (2008). 'Information systems continuance intention of web-based applications customers: the case of online banking', *Information & Management*, 45*(7)*, pp. 419-428.

Venkatesh, V., Brown, S. & Bala, H. (2013). 'Bridging the qualitative-quantitative divide: guidelines for conducting mixed methods research in information systems', *MIS Quarterly*, 37*(1)*, pp. 21-54.

Venkatesh, V., Morris, M.G., Davis, G.B. & Davis, F.D. (2003). 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, 27*(3)*, pp. 425-478.

Venkatesh, V., Thong, J. & Xu, X. (2012). 'Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology', *MIS Quarterly*, 36*(1)*, pp. 157-178.

Venktess, K. (2017). *Cybercrime to cost business up to R78 trillion in four years*, available from: https://www.fin24.com/Tech/Cyber-Security/cybercrime-to-cost-business-up-to-r78-trillion-in-four-years-20170307, Fin24, Johannesburg, [last accessed: 25 January 2018].

Von Solms, R. & Von Solms, S. (2014). 'Towards cyber safety education in primary schools in Africa', *Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance*, International Institute of Informatics and Systemics, Plymouth, 8-9 July, pp. 185-197.

Walker, J. (2014). 'Internet Security', In: J.R. Vacca (ed.), *Network and System Security*, 2nd ed., pp. 179-220, Elsevier, Waltham, MA.

Walton, D. (2014). *Abductive Reasoning*, University of Alabama Press, Tuscaloosa, AL.

Weirich, D. & Sasse, M.A. (2001). 'Pretty good persuasion: a first step towards effective password security in the real world', *Proceedings of the 2001 Workshop on New Security Paradigms*, ACM, Cloudcroft, NM, 11-13 September, pp. 137-143.

Werner, C. & Schermelleh-Engel, K. (2009). *Introduction to Structural Equation Modeling with LISREL*, Goethe University, Frankfurt.

Whitman, M. & Mattord, H. (2017). *Principles of Information Security*, 6th ed., Cengage Learning, Boston, MA.

Whitten, A. & Tygar, J.D. (1999). ‘Why Johnny can’t encrypt: a usability evaluation of PGP 5.0’, *Proceedings of the 8th USENIX Security Symposium*, USENIX, Washington, D.C., 23-26 August, pp. 169-184.

Williams, B., Onsman, A. & Brown, T. (2010). ‘Exploratory factor analysis: a five-step guide for novices’, *Australasian Journal of Paramedicine*, 8*(3)*, pp. 1-13.

Wolfswinkel, J.F., Furtmueller, E. & Wilderom, C.P.M. (2011). ‘Using grounded theory as a method for rigorously reviewing literature’, *European Journal of Information Systems*, 22*(1)*, pp. 45-55.

Xiong, A., Proctor, R.W., Yang, W. & Li, N. (2017). ‘Is domain highlighting actually helpful in identifying phishing web pages?’, *Human factors*, 59*(4)*, pp. 640-660.

Yee, K.P. (2005). ‘Guidelines and strategies for secure interaction design’, In: L.F. Cranor & S. Garfinkel (eds.), *Security and Usability: Designing Secure Systems That People Can Use*, pp. 253-279, O’Reilly Media, Sebastopol, CA.

Yee, K.P. (2004a). ‘Aligning security and usability’, *IEEE Security & Privacy*, 1*(5)*, pp. 48-55.

Yee, K.P. (2004b). ‘Secure interaction design’, *Proceedings of the 8th International Conference on Financial Cryptography*, ICFC, Key West, FL, 9-12 February, pp. 114-115.

ACM, Fort Lauderdale, FL, 5-10 April, .

Yee, K.P. (2002). ‘User interaction design for secure systems’, *Proceedings of the 4th International Conference on Information and Communications Security*, ICICS, Singapore, 9-12 December, pp. 278-290.

Yeratziotis, A., Pottas, D. & Van Greunen, D. (2012). ‘A usable security heuristic evaluation for the online health social networking paradigm’, *International Journal of Human-Computer Interaction*, 28*(10)*, pp. 678-694.

Yin, R.K. (2016). *Qualitative Research from Start to Finish*, 2nd ed., Guilford Press, New York, NY.

Yin, R.K. (2014). *Case Study Research: Design and Methods*, 5th ed., Sage Publications, Thousand Oaks, CA.

Yousafzai, S.Y., Pallister, J.G. & Foxall, G.R. (2003). ‘A proposed model of e-trust for electronic banking’, *Technovation*, 23*(11)*, pp. 847-860.

Yousafzai, S.Y. & Yani-de-Soriano, M. (2012). ‘Understanding customer-specific factors underpinning internet banking adoption’, *International Journal of Bank Marketing*, 30*(1)*, pp. 60-81.

Zafar, H. & Clark, J.G. (2009). 'Current state of information security research in IS', *Communications of the Association for Information Systems*, 24*(1)*, pp. 571-596.

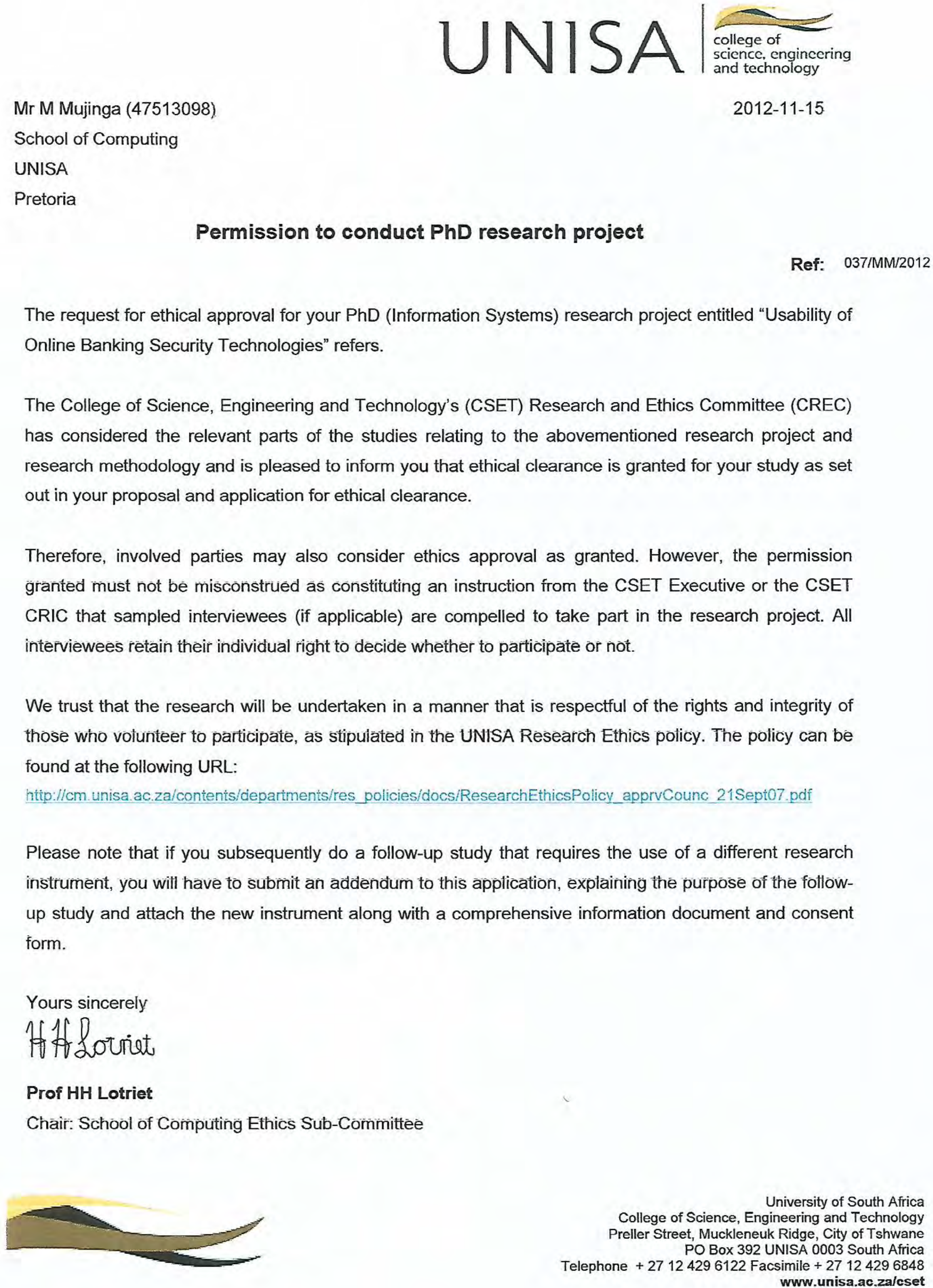
Zahidi, Z., Lim, Y.P. & Woods, P.C. (2014). 'Understanding the user experience (UX) factors that influence user satisfaction in digital culture heritage online collections for non-expert users', *Proceedings of the Science and Information Conference*, IEEE, London, 27-29 August, pp. 57-63.

Zargar, S.T., Joshi, J. & Tipper, D. (2013). 'A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks', *IEEE Communications Surveys & Tutorials*, 15*(4)*, pp. 2046-2069.

Zhuang, W., Hsu, M.K., Brewer, K.L. & Xiao, Q. (2012). 'Paradoxes of social networking sites: an empirical analysis', *Management Research Review*, 36*(1)*, pp. 33-49.

APPENDICES

APPENDIX A: Ethical certificates



UNISA | college of science, engineering and technology

Mr M Mujinga (47513098)
School of Computing
UNISA
Pretoria

2012-11-15

Permission to conduct PhD research project

Ref: 037/MM/2012

The request for ethical approval for your PhD (Information Systems) research project entitled "Usability of Online Banking Security Technologies" refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CRIC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

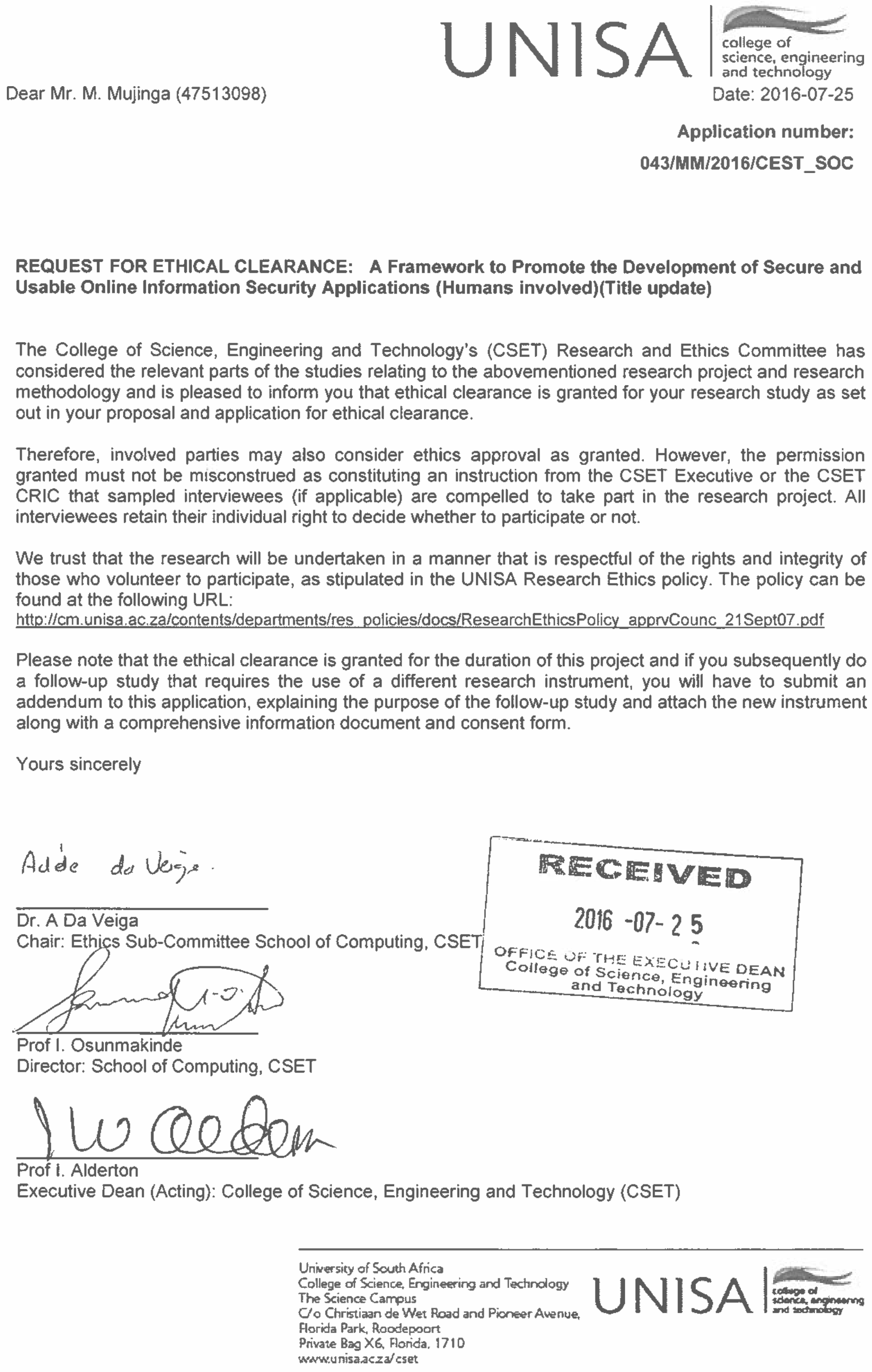
Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

H H Lotriet

Prof HH Lotriet
Chair: School of Computing Ethics Sub-Committee

University of South Africa
College of Science, Engineering and Technology
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone + 27 12 429 6122 Facsimile + 27 12 429 6848
www.unisa.ac.za/cset



UNISA | college of science, engineering and technology

Dear Mr. M. Mujinga (47513098)

Date: 2016-07-25

Application number:

043/MM/2016/CEST_SOC

REQUEST FOR ETHICAL CLEARANCE: A Framework to Promote the Development of Secure and Usable Online Information Security Applications (Humans involved)(Title update)

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your research study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CRIC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:
http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

Please note that the ethical clearance is granted for the duration of this project and if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

Adele da Veiga

Dr. A Da Veiga
Chair: Ethics Sub-Committee School of Computing, CSET

Prof I. Osunmakinde
Director: School of Computing, CSET

Prof I. Alderton
Executive Dean (Acting): College of Science, Engineering and Technology (CSET)

PROF L LABUSCHAGNE
EXECUTIVE DIRECTOR: RESEARCH DEPARTMENT
***Tel**: +27 12 429 6368 / 2446*
***Email**: llabus@unisa.ac.za*
***Address**: Theo van Wijk Building, 10th Floor, Office no. 50 (TvW 10-50)*

10 July 2014

Mr M Mujinga
School of Computing
College of Science, Engineering and Technology

Dear Mr Mujinga

PERMISSION TO DO RESEARCH INVOLVING UNISA STAFF, STUDENTS OR DATA

A study into "Usability of online banking security technologies"

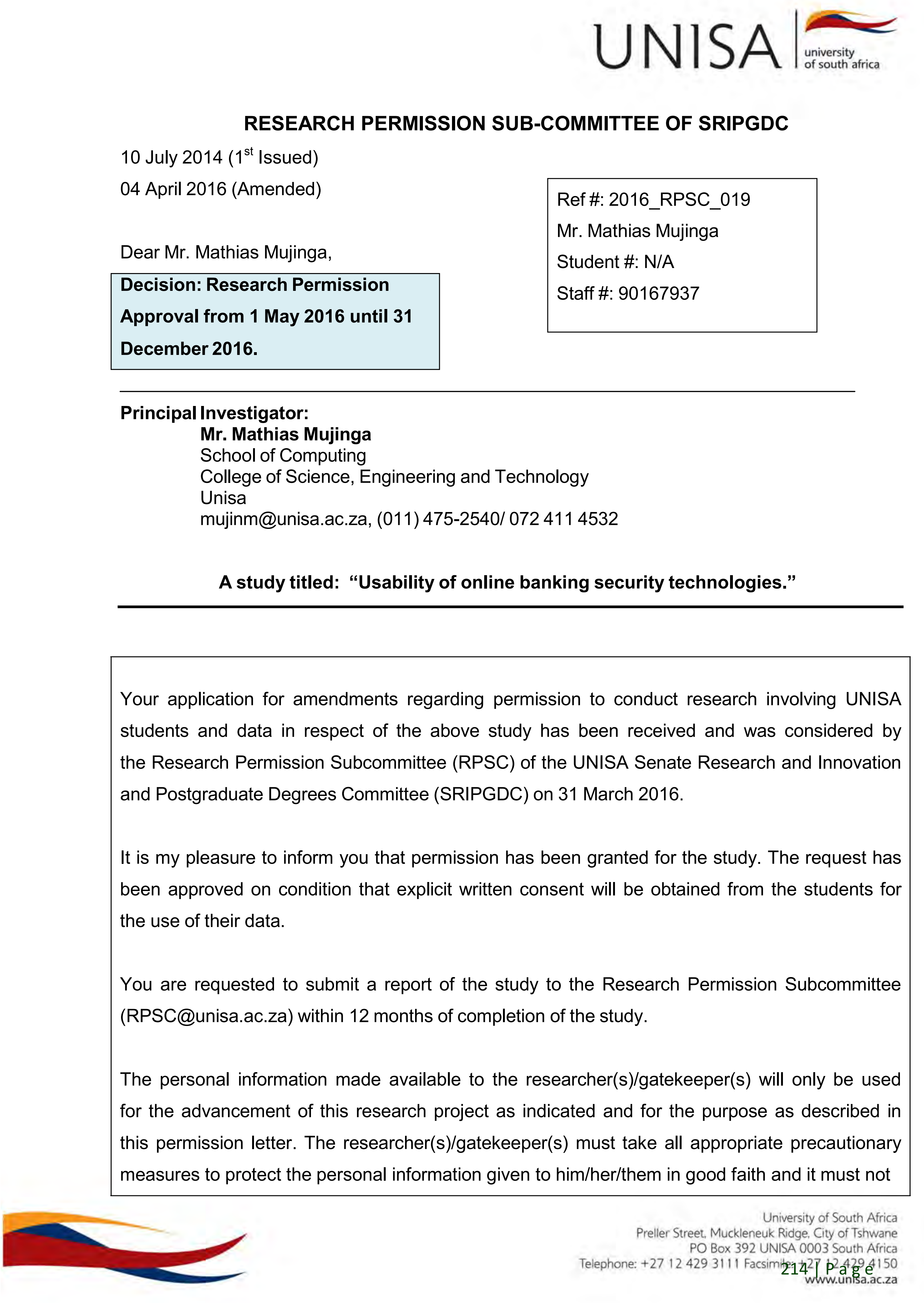
Your application regarding permission to conduct research involving Unisa staff, students or data in respect of the above study has been received and was considered by the Unisa Senate Research and Innovation and Higher Degrees Committee (SRIHDC) on 05 June 2014.

It is my pleasure to inform you that permission has been granted for this study as set out in your application.

We would like to wish you well in your research undertaking.

Kind regards

PROF L LABUSCHAGNE
EXECUTIVE DIRECTOR: RESEARCH



RESEARCH PERMISSION SUB-COMMITTEE OF SRIPGDC

10 July 2014 (1st Issued)

04 April 2016 (Amended)

Ref #: 2016_RPSC_019
Mr. Mathias Mujinga
Student #: N/A
Staff #: 90167937

Dear Mr. Mathias Mujinga,

Decision: Research Permission Approval from 1 May 2016 until 31 December 2016.

Principal Investigator:
Mr. Mathias Mujinga
School of Computing
College of Science, Engineering and Technology
Unisa
mujinm@unisa.ac.za, (011) 475-2540/ 072 411 4532

A study titled: "Usability of online banking security technologies."

Your application for amendments regarding permission to conduct research involving UNISA students and data in respect of the above study has been received and was considered by the Research Permission Subcommittee (RPSC) of the UNISA Senate Research and Innovation and Postgraduate Degrees Committee (SRIPGDC) on 31 March 2016.

It is my pleasure to inform you that permission has been granted for the study. The request has been approved on condition that explicit written consent will be obtained from the students for the use of their data.

You are requested to submit a report of the study to the Research Permission Subcommittee (RPSC@unisa.ac.za) within 12 months of completion of the study.

The personal information made available to the researcher(s)/gatekeeper(s) will only be used for the advancement of this research project as indicated and for the purpose as described in this permission letter. The researcher(s)/gatekeeper(s) must take all appropriate precautionary measures to protect the personal information given to him/her/them in good faith and it must not be passed on to third parties.

Note:

*The reference number **2016_RPSC_019** should be clearly indicated on all forms of communication with the intended research participants and the Research Permission Subcommittee.*

We would like to wish you well in your research undertaking.

Kind regards,

Prof L Labuschagne – Chairperson: RPSC

Email: llabus@unisa.ac.za

Tel: (012) 429-6368

Appendix B: Consent forms – Survey

Respondent Number: _____________

Letter of informed consent to be signed by all respondents

Research Project: **USABILITY OF ONLINE BANKING SECURITY TECHNOLOGIES**

Researcher: Mr. M. Mujinga

Promoter: Prof. MM Eloff

Co-Promoter: Prof. JH Kroeze

School of Computing

College of Science, Engineering and Technology

University of South Africa

Dear Prospective Respondent

My name is Mathias Mujinga and I am doing research with Prof MM Eloff (Research Professor: Institute for Corporate Citizenship) and Prof JH Kroeze (Chair, Department: School of Computing) towards a PhD in Computer Science at the University of South Africa. I am inviting you to participate in a study entitled "USABILITY OF ONLINE BANKING SECURITY TECHNOLOGIES". I am requesting your participation in this study. The research was reviewed and approved by the Research Ethics Committee of the College of Science, Engineering and Technology, Unisa. The study looks at the usability aspects of online banking security service, particularly; the design, development and human-related aspects of online banking websites and how these aspects affect the effective use of such service. Your participation will be in the form of a questionnaire respondent.

Data collected will remain confidential, but it can only be disposed after five years because of the university rules. After five years all material used in this survey will be destroyed.

The questionnaire will take a maximum of ten (10) minutes to complete. Should you wish to participant in this study; please fill in and sign the section below

I ____ (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire. I hereby give permission that my responses may be used in the above research project, provided that none of my personal details will be made public in the published research report.

Should you wish to complete the online version of the questionnaire please click the button below:

Take Online Survey Here

Signature: ______________________________ **Date:** _______________

Place: __________________________________

COVER LETTER TO AN ONLINE ANONYMOUS WEB-BASED SURVEY

Dear Prospective Respondent,

You are invited to participate in a survey conducted by Mathias Mujinga for the research project entitled: “Usability of Online Banking Security Technologies” under the supervision of Prof MM Eloff (Research Professor: Institute for Corporate Citizenship) and Prof JH Kroeze (Chair, Department: School of Computing towards a PhD in Computer Science at the University of South Africa.

The survey you have received has been designed to study the user acceptance and usability evaluation of online banking service in South Africa. You were selected to participate in this survey because you use online banking service provided by a South African bank. You will not be eligible to complete the survey if you do not use online banking service provided by any of the South African banks. By completing this survey, you agree that the information you provide may be used for research purposes only, including dissemination through peer-reviewed publications and conference proceedings.

It is anticipated that the information we gain from this survey will help us to develop a framework for the design of secure and usable online banking service. You are, however, under no obligation to complete the survey and you can withdraw from the study prior to submitting the survey. The survey is developed to be anonymous, meaning that we will have no way of connecting the information that you provide to you personally. Consequently, you will not be able to withdraw from the study once you have clicked the send button based on the anonymous nature of the survey. If you choose to participate in this survey it will take up no more than 15 minutes of your time. You will not benefit from your participation as an individual, however, it is envisioned that the findings of this study will shed light into the design of online banking services to improve the security of the service by making it more user-friendly. We do not foresee that you will experience any negative consequences by completing the survey. The researcher(s) undertake to keep any information provided herein confidential, not to let it out of our possession and to report on the findings from the perspective of the participating group and not from the perspective of an individual.

The records will be kept for five years for audit purposes where after it will be permanently destroyed. Hard copies will be shredded and electronic versions will be permanently deleted from the hard drives of any computers used. You will not be reimbursed or receive any incentives for your participation in the survey.

The research was reviewed and approved by the Research Ethics Committee of the College of Science, Engineering and Technology, Unisa. The primary researcher, Mathias Mujinga, can be contacted during office hours at mujinm@unisa.ac.za and 011 471 3154. The study leaders can be contacted during office hours at: Prof MM Eloff (eloffmm@unisa.ac.za and 012 433 4604) and Prof JH Kroeze (kroezjh@unias.ac.za and 011 670 9117). Should you have any questions regarding the ethical aspects of the study, you can contact the chairperson of the Research Ethics Committee of the College of Science, Engineering and Technology, Prof E Mnkandla during office hours at mnkane@unisa.ac.za and 011 670 9059. Alternatively, you can report any serious unethical behaviour at the University's Toll Free Hotline 0800 86 96 93.

You are making a decision whether or not to participate by opening the survey link. You are free to withdraw from the study at any time prior to clicking the send button.

Appendix C: Consent forms – Interviews

UNISA university of south africa

Respondent Number: _____________

Letter of informed consent to be signed by all participants

Research Project: **A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS**

Researcher: Mr. M. Mujinga

Promoter: Prof. MM. Eloff

Joint Promoter: Prof. JH. Kroeze

School of Computing, College of Science, Engineering and Technology

University of South Africa

Dear Prospective participant

I am conducting research for my PhD studies on the usability of online banking security; I am requesting your participation in this study. The study investigates the usability aspects of online banking security technology, particularly; the design, development and human-related aspects of online banking security tools and how these aspects affect the effective use of such tools. Your participation will be in the form of an interview and the interview will take a maximum of one (1) hour to complete.

Interviews will be recorded using a digital recorder. Data collected during the interview will remain confidential, but it can only be disposed after five years because of the university rules. After five years all material used in this interview will be destroyed.

Anonymity of the participants will be strictly protected and all data collected from the participants will be treated with full confidentiality. Please note that only the researcher, promoter and joint promoter will have access to the data collected at any point in time during the course of the research.

Should you agree to participant in this study, please fill in and sign the section below

I ____ (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire. I hereby give permission that my responses may be used in the above research project, provided that none of my personal details will be made public in the published research report.

Signature: _____________________________ **Date:** _______________

Place: __________________________________

PARTICIPANT’S INFORMATION SHEET

Dear Prospective Participant

My name is Mathias Mujinga and I am doing research with Prof MM Eloff (Research Professor: Institute for Corporate Citizenship) and Prof JH Kroeze (Chair, Department: School of Computing) towards a PhD in Computer Science at the University of South Africa. We are inviting you to participate in a study entitled “A Framework to Promote the Development of Secure and Usable Online Information Security Applications”.

WHAT IS THE PURPOSE OF THE STUDY?

The aim of this research is to develop a framework for secure and usable online banking service. I am conducting this research to investigate the current standards for design and development of online banking websites and investigate the general usability of this service to the user. We intend to develop a framework that incorporates user interface design principles that cater for security, usability and user experience goals.

WHY ARE YOU BEING INVITED TO PARTICIPATE?

I need to interview at least one member of the ICT sections of all four major South African banks and you have been chosen to represent your bank.

I obtained your contact details from **<name>** and I invite you to participate in this research as you are currently working with ICT systems at **<bank name>**. I believe you can contribute to the current state of South African online banking security and their improved usability and user experience for clients by answering the questions posed in this study.

WHAT IS THE NATURE OF YOUR PARTICIPATION IN THIS STUDY?

The study involves the initial audio-recording of your responses to semi-structured interviews with the likelihood of scheduling another follow-up interview. Your exact role in the interview for the research will be to answer the questions. The interview will take a maximum of one hour and will be scheduled at your convenience and at a location of your choice.

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

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason. During the interview session you can also decide not to answer any specific question without giving a reason.

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

The results of this study have the potential to assist the stakeholders with the development of online banking services that are user-friendly, which in turn fosters effective use and encourage adoption of the service. Potential stakeholders that are set to benefit from this research are financial institutions and online banking users.

ARE THEIR ANY NEGATIVE CONSEQUENCES FOR YOU IF YOU PARTICIPATE IN THE RESEARCH PROJECT?

The anticipated inconvenience will be finding the time to conduct the interview, hence the recommendation that you choose the time and place for the interview.

WILL THE INFORMATION THAT YOU CONVEY TO THE RESEARCHER AND YOUR IDENTITY BE KEPT CONFIDENTIAL?

Please note that your name will not be recorded anywhere and no one will be able to connect you to your answers as you will be given a fictitious participant code associated with your responses. This code also applies to any publications or other research report methods such as presentations at conferences.

Your answers will only be reviewed by people responsible for ensuring that research is done properly, including research promoters (supervisors), a transcriber, an external coder and members of the Research Ethics Committee. Therefore, the records that identify you will be available strictly to people working on the study, unless you give permission for other people to see the records.

A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report. Results will also be published in the thesis, which will be available on the Unisa Institutional Repository.

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

Interview recording digital files will be stored by the researcher for a period of five years on a password protected computer/hard drive. Future use of the stored data will be subject to a further Research Ethics Review and approval, if applicable. All data and information (documents and tape recorders) collected during the course of this research will be incinerated after five years.

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

We do not provide any financial benefit for participation, but you are given an opportunity to have your say and contribute towards enhancing the current state of online banking service.

HAS THE STUDY RECEIVED ETHICAL APPROVAL?

This study has received written approval from the Research Ethics Committee of the College of Science, Engineering and Technology, Unisa. A copy of the approval letter is attached to this information pack. Please do not hesitation to contact the researcher or any of the provided contacts for more information and clarity with regard to ethical issues.

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

If you would like to be informed of the final research findings, please contact Mathias Mujinga on 011 471 3154 or mujinm@unisa.ac.za. The findings are accessible for a period of two (2) years after completion of the research.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact him via the same telephone number or e-mail address. Should you have concerns about the way in which the research has been conducted, you may contact the study leaders Prof MM Eloff and Prof JH Kroeze via the contact details given below.

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

MATHIAS MUJINGA

PhD Candidate (UNISA) | mujinm@unisa.ac.za | 011 471 3154

PROMOTERS:

Prof MM Eloff (UNISA) | eloffmm@unisa.ac.za | 012 433 4604

Prof JH Kroeze (UNISA) | kroezjh@unisa.ac.za | 011 670 9117

Participant Number: ____________

CONSENT TO PARTICIPATE IN THIS STUDY

RESEARCH TITLE: A FRAMEWORKTO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS

I, ___________________________ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable)

I am aware that the findings of this study will be anonymously processed into a research report, journal publications, and/or conference proceedings.

I agree to the recording of the semi-structured interviews.

I have received a signed copy of the informed consent agreement.

I have received a written approval from the Research Ethics Committee of the College of Science, Engineering and Technology, UNISA.

Participant Name & Surname……………………………………...……… (please print)

Participant

Signature………………………………………..Date…………………….……………

Researcher's Name & Surname………………………...……..………... (please print)

Researcher's

Signature……………………………………Date………………………………

Witness Name & Surname.. (please print)

Witness's

Signature…………………………….............Date…...

Appendix D: Consent form – Evaluation tool

Participant Number: _____________

Letter of informed consent to be signed by all participants

Research Project:

A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS

Researcher: Mr. M. Mujinga

Promoter: Prof. MM Eloff

Co-Promoter: Prof. JH Kroeze

School of Computing

College of Science, Engineering and Technology

University of South Africa

Dear Prospective Participant

My name is Mathias Mujinga and I am doing research with Prof MM Eloff (Research Professor: Institute for Corporate Citizenship) and Prof JH Kroeze (Professor: School of Computing) towards a PhD in Computer Science at the University of South Africa. We are inviting you to participate in a study entitled "A Framework to Promote the Development of Secure and Usable Online Information Security Applications". I am requesting your participation in this study. The research was reviewed and approved by the Research Ethics Committee of the College of Science, Engineering and Technology, Unisa. The study looks at the usability aspects of online banking security service, particularly; the design, development and human-related aspects of online banking websites and how these aspects affect the effective use of such service. Your participation will be in the form of an evaluator.

Data collected will remain confidential, but it can only be disposed after five years because of the university rules. After five years all material used in this evaluation will be destroyed.

The evaluation will take a maximum of thirty (30) minutes to complete. Should you wish to participant in this study; please fill in and sign the section below

I ____ (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire. I hereby give permission that my responses may be used in the above research project, provided that none of my personal details will be made public in the published research report.

Signature: ________________________________ **Date:** ________________

Place: ____________________________________

PARTICIPANT’S INFORMATION SHEET

Dear Prospective Participant

My name is Mathias Mujinga and I am doing research with Prof MM Eloff (Research Professor: Institute for Corporate Citizenship) and Prof JH Kroeze (Professor: School of Computing) towards a PhD in Computer Science at the University of South Africa. We are inviting you to participate in a study entitled “A Framework to Promote the Development of Secure and Usable Online Information Security Applications”.

WHAT IS THE PURPOSE OF THE STUDY?

The aim of this research is to develop a framework for secure and usable online banking service. I am conducting this research to investigate the current standards for design and development of online banking websites and investigate the general usability of this service to the user. We intend to develop a framework that incorporates user interface design principles that cater for security, usability and user experience goals.

WHY ARE YOU BEING INVITED TO PARTICIPATE?

You have been chosen due to your expert knowledge in the field of security and usability. I obtained your contact details from [NAME] and I invite you to participate in this research as you are currently working with ICT systems. I believe you can contribute to the validation of the proposed framework and the current state of online banking service in South Africa.

WHAT IS THE NATURE OF YOUR PARTICIPATION IN THIS STUDY?

I request your participation as a field expert in the evaluation of the 12 selected design principles for secure and usable online banking interface. Each of the principles consists of between 3 and 9 checklist items where we need your input in determining the relevance and importance to the proposed framework. The exercise will take a maximum of 60 minutes of your time. We would appreciate it if you could return your evaluation report within 2 weeks of receiving the relevant documentation.

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

Participating in this study is voluntary and you are under no obligation to consent to participation. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason.

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

The results of this study have the potential to assist the stakeholders with the development of online banking services that are user-friendly, which in turn fosters effective use and encourage adoption of the service. Potential stakeholders that are set to benefit from this research are financial institutions and online banking users.

ARE THEIR ANY NEGATIVE CONSEQUENCES FOR YOU IF YOU PARTICIPATE IN THE RESEARCH PROJECT?

The anticipated inconvenience will be finding the time to complete the evaluation exercise, hence we have given you 2 weeks to return the completed evaluation tool. You are welcome to request more time if this time frame is not conducive to your schedule.

WILL THE INFORMATION THAT YOU CONVEY TO THE RESEARCHER AND YOUR IDENTITY BE KEPT CONFIDENTIAL?

Please note that your name will not be recorded anywhere and no one will be able to connect you to your answers as you will be given a fictitious participant code associated with your responses. This code also applies to any publications or other research report methods such as presentations at conferences.

Your answers will only be reviewed by people responsible for ensuring that research is done properly, including research promoters (supervisors) and members of the Research Ethics Committee at Unisa. Therefore, the records that identify you will be available strictly to people working on the study, unless you give permission for other people to see the records.

A report of the study may be submitted for publication, but individual participants will not be identifiable in such a report. Results will also be published in the thesis, which will be available on the Unisa Institutional Repository.

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

Participants' responses in digital format will be stored by the researcher for a period of five years on a password protected computer and hard drive. Future use of the stored data will be subject to a further Research Ethics Review and approval, if applicable. All data and information in physical format collected during the course of this research will be incinerated after five years.

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

We do not provide any financial benefit for participation, but you are given an opportunity to have your say and contribute towards enhancing the current state of online banking service.

HAS THE STUDY RECEIVED ETHICAL APPROVAL?

This study has received written approval from the Research Ethics Committee of the College of Science, Engineering and Technology, Unisa. A copy of the approval letter is attached to this information pack. Please do not hesitate to contact the researcher or any of the provided contacts for more information and clarity with regard to ethical issues.

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

If you would like to be informed of the final research findings, please contact Mathias Mujinga on mujinm@unisa.ac.za. The findings are accessible for a period of two (2) years after completion of the research.

Should you require any further information or want to contact the researcher about any aspect of this study, please contact him via the same telephone number or e-mail address. Should you have concerns about the way in which the research has been conducted, you may contact the study leaders Prof MM Eloff and Prof JH Kroeze via the contact details given below.

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

MATHIAS MUJINGA

PhD Candidate (UNISA) | mujinm@unisa.ac.za | 011 471 3154

PROMOTERS:

Prof MM Eloff (UNISA) | eloffmm@unisa.ac.za | 012 433 4604

Prof JH Kroeze (UNISA) | kroezjh@unisa.ac.za | 011 670 9117

Participant Number: _____________

CONSENT TO PARTICIPATE IN THIS STUDY

RESEARCH TITLE: A FRAMEWORKTO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS

I, ____________________________ (participant name), confirm that the person asking my consent to take part in this research has told me about the nature, procedure, potential benefits and anticipated inconvenience of participation.

I have read (or had explained to me) and understood the study as explained in the information sheet.

I have had sufficient opportunity to ask questions and am prepared to participate in the study.

I understand that my participation is voluntary and that I am free to withdraw at any time without penalty (if applicable).

I am aware that the findings of this study will be anonymously processed into a research report, journal publications, and/or conference proceedings.

I agree to the recording of the semi-structured interviews.

I have received a signed copy of the informed consent agreement.

I have received a written approval from the Research Ethics Committee of the College of Science, Engineering and Technology, UNISA.

Participant Name & Surname………………………………………….……… (please print)

Participant

Signature…………………………………..Date……………….………………

Researcher's Name & Surname…………………………...……..….... (please print)

Researcher's

Signature…………………………………Date………………………………

Witness Name & Surname.. (please print)

Witness's

Signature………………………...............Date…..

Appendix E: Online banking evaluation survey

The purpose of this survey is to obtain user acceptance and usability evaluation of online banking services in South Africa. The questions are based on the views of the users about their respective banks' online banking websites (user interfaces). Please answer the questions to the best of your knowledge. All the information provided in this survey will be strictly confidential and will be used for research purposes only. Respondents' identities are not collected and they will remain confidential and will not be published in any way. The survey will take you approximately 10 minutes to complete.

Consent Form

Please note that by submitting this form you agree that you have not been put under any pressure to participate in this evaluation exercise and have willingly participated in it. Also, please note that participation is voluntary and that you may withdraw at any time without negative consequences. Please understand that the findings of the evaluation will be used for research purposes only and may be published in academic publications. Your privacy will be protected by not printing any names, position or institution in any such publication. Your answers to these questions will be used for academic purposes only. The data will be stored for five years at UNISA, after which it will be destroyed.

Please tick the check box to voluntarily provide consent to participate in the study □

Indicate your choice by marking the appropriate blank block next to a number with an 'X'.

SECTION A: Demographic details

A1: Gender:

Male	1	
Female	2	

A2: Age:

Younger than 20 years	1	
20–29 years	2	
30–39 years	3	
40–49 years	4	
50 years or older	5	

A3: Home language (specify): ________________

A4: Highest educational qualification:

No formal education	1	
Matric	2	
Post-matric certificate or diploma	3	
Degree	4	
Postgraduate degree	5	
Other (specify below)	6	

A5: Employment status:

Employed	1	
Self-employed	2	
Unemployed	3	
Retired	4	
Other (specify below)		

A6: Income per month before tax and other deductions:

Less than R10 000	1	
R10 000 – R19 999	2	
R20 000 – R29 999	3	
R30 000 – R39 999	4	
R40 000 – R49 999	5	
R50 000 or more	6	

A7: South African province (your current location):

Eastern Cape	1	
Free State	2	
Gauteng	3	
KwaZulu-Natal	4	
Limpopo	5	
Mpumalanga	6	
North West	7	
Northern Cape	8	
Western Cape	9	

A8: Ethnic group:

Black	1	
White	2	
Coloured	3	
Indian/Asian	4	
Other (specify below)	5	

SECTION B: General questions

B9: Please choose *ONLY ONE* South African bank that you use most for online banking and answer the rest of the questions based on the selected bank:

ABSA	1	
Capitec	2	
FNB	3	
Investec	4	
Nedbank	5	
Standard Bank	7	
Other (specify below)	8	

B10: How long have you been using online banking?

Less than 12 months	1	
1–2 years	2	
3–4 years	3	
5–6 years	4	
7 years or more	5	

B11: How often do you use online banking?

Every day	1	
Once a week	2	
Once every two weeks	3	
Once a month	4	
Other (specify below)	5	

B12: Which device(s) do you use to connect to online banking? (*Please select ALL that apply.*)

Computer (at home)	1	
Computer (at work)	2	
Public computer (Internet café)	3	
Laptop/portable device	4	
Mobile device	5	
Other (specify below)	6	

SECTION C: ACCEPTANCE AND USE

Please select the extent to which you disagree or agree with the following statements with regard to your chosen bank's online banking service:	**Strongly disagree** **1**	**Disagree** **2**	**Neutral** **3**	**Agree** **4**	**Strongly agree** **5**
Performance Expectancy					
a. I find online banking useful in my daily life					
b. Using online banking helps me accomplish things more quickly					
c. Using online banking increases my productivity					
d. Online banking saves me time when I use it					
e. Online banking does everything I would expect it to do					
Effort Expectancy					
f. I find online banking easy to use					
g. It is easy for me to become skilful at using online banking					
h. Interacting with the online banking website does not require a lot of mental effort					
i. I can use online banking without written instructions					
j. Using online banking is effortless					
k. Online banking is user friendly					
Social Influence					
l. People who influence my behaviour think that I should use online banking					
m. People who are important to me think that I should use online banking					
n. People whose opinions I value recommend that I use online banking					
o. Using online banking is a status symbol in my life					
Facilitating Conditions					
p. I have the resources necessary to use online banking					
q. I have the knowledge necessary to use online banking					
r. Online banking works well with other technologies I use					
s. I can get help from others when I have difficulties using online banking					
Hedonic Motivation					
t. Using online banking is fun					
u. Using online banking is enjoyable					
v. Using online banking is entertaining					
w. The actual process of using online banking is pleasant					
Price Value					
x. Online banking is reasonably priced					
y. Online banking is good value for money					
z. At the current price, online banking provides good value					
Habit					
aa. The use of online banking has become a habit for me					
bb. I am addicted to using online banking					
cc. I must use online banking					
dd. Assuming I had access to online banking, I intend to use it					
ee. Given that I have internet access, I predict that I will continue using online banking					
Behavioural Intention					
ff. I intend to continue using online banking in the future					
gg. I will always try to use online banking regularly					
hh. I plan to increase the frequency of using online banking					

SECTION D: Usability

Please select the extent to which you disagree or agree with the following statements with regard to your chosen bank's online banking service:	**Strongly disagree** **1**	**Disagree** **2**	**Neutral** **3**	**Agree** **4**	**Strongly agree** **5**
The System Usability Scale					
a. I think that I would like to use online banking more frequently					
b. I find online banking unnecessarily complex					
c. I need the support of a technical person, to be able to use online banking					
d. I found the various functions in online banking to be well integrated					
e. I thought there was too much inconsistency in online banking					
f. I would imagine that most people would learn to use online banking websites very quickly					
g. I find online banking very difficult to use					
h. I feel confident using online banking					

i. I needed to learn a lot of things before I could get going with online banking					
j. I thought online banking was easy to use					

Please select the extent to which you disagree or agree with the following statements with regard to your chosen bank's online banking service:	**Strongly disagree** **1**	**Disagree** **2**	**Neutral** **3**	**Agree** **4**	**Strongly agree** **5**
Learnability					
k. Learning how to use online banking is easy for me					
l. I learned easily to use online banking the first time I logged in					
m. I quickly became competent in using online banking					
n. The abbreviations used are easy to remember					
o. My interaction with the online banking website is clear and understandable					
User Suitability					
p. I understand the language used on the online banking website					
q. The online banking website allows me to choose my preferred language					
r. I think both regular and new users would like using online banking					
Satisfaction					
s. I am satisfied with using online banking					
t. Online banking works the way I want it to work					
u. I would recommend online banking to others					
v. I feel I need to have online banking					
w. Online banking is wonderful					
Availability					
x. The online banking website is always available					
y. The online banking transactions are always available					
z. There are frequent scheduled system downtimes					
aa. Internet connection problems prevent access to online banking					
bb. Frequent online banking website changes are confusing					
Errors					
cc. The online banking service error messages do not interfere with my online activity					
dd. The online banking service error messages are informative					
ee. The online banking service error messages highlight problem fields					
ff. I can recover from mistakes quickly and easily					
gg. The online banking service asks for user confirmation on irreversible actions					
Help and Documentation					
hh. The online banking service has a HELP function					
ii. The online banking service indicates the transaction processing status					
jj. The bank offered me training when I registered for online banking					
kk. I still need training on how to use online banking					
ll. The bank keeps me informed on the risks of using online banking					
mm. The online banking service provides a search option for locating functions					

SECTION E: Security AND PRIVACY

Please select the extent to which you disagree or agree with the following statements with regard to your chosen bank's online banking service:	**Strongly disagree** **1**	**Disagree** **2**	**Neutral** **3**	**Agree** **4**	**Strongly agree** **5**
a. Using online banking is financially secure					
b. I trust in the ability of my online banking service to protect my privacy					
c. I trust in the technology my online banking service is using					
d. I trust my online banking service in the same way that I trust my bank's branch					
e. I am not worried about the security of my online banking service					
f. Matters of security have no influence on my use of online banking					
g. I am confident that online banking in South Africa is secure					
h. I feel safe when I send personal information to the online banking website					
i. I trust that the online banking website only collects users' personal data that is necessary for its activities					
j. I trust that the online banking website will not provide my personal information to other companies without my consent					
k. I trust that the online banking website has sufficient technical capacity to ensure that the data I send will not be intercepted by hackers					

l. The online banking website has a good reputation compared to other rival banks' websites					
m. The online banking website keeps users informed about the security status					

SECTION F: OVERALL ASSESSMENT

1. Overall, what do you like most about online banking?

1	
2	
3	
4	
5	
6	

2. Overall, what are your main concerns about online banking?

1	
2	
3	
4	
5	
6	

3. Do you have any additional comments with regard to your experience of using online banking?

____

____

____

____

____

____

____

THANK YOU VERY MUCH FOR YOUR PARTICIPATION

Mr M Mujinga, School of Computing, College of Science, Engineering and Technology, UNISA | mujinm@unisa.ac.za

Prof MM Eloff, Institute for Corporate Citizenship, College of Economic and Management Sciences, School of Computing, UNISA (Promoter)

Prof JH Kroeze, School of Computing, College of Science, Engineering and Technology, UNISA (Co-promoter)

Appendix F: Interview questions

Section A: Biographical information

Participant number				
Gender	Male		Female	
Age				
Ethnicity				
Province				
Home language				
Highest qualification				
Bank				
Position in bank			Specialisation	
Years in position				

Section B: Online banking service

1. Does the bank offer new online banking (OB) clients training on how to use the service?
2. Does the bank provide a 24-hour help desk specifically to assist OB and other digital channels' clients?
3. Do clients report any specific challenges when it comes to using OB and other digital channels?
4. Does the bank charge a monthly subscription fee for using OB?
5. Does the bank charge a fee for individual OB transactions?
6. Does the bank have initiatives to encourage the usage of OB and other digital channels?
7. Does the bank plan on scaling down on branch operations (reducing branches and branch staff), following the trend of other international banks?
8. Can clients suggest/request certain OB capabilities for consideration?
9. What responsibilities do OB clients have to protect their OB transactions from interception?
10. Are these responsibilities communicated to clients upon OB adoption? If yes, how?
11. What communication strategies are used to communicate with OB clients?

Section C: Online banking system development

12. Does the bank develop OB systems internally or externally (outsourced)?
13. Does the development of OB systems/services take input from users of the system?
14. Which (if any) development standards do you follow internationally or locally?
15. What software engineering/application development principles/frameworks are followed for OB design and development?
16. What IT management and governance frameworks are followed in OB development?
17. What information security management frameworks are followed in OB development?
18. Do you incorporate any usability and user experience design principles in the development of OB?

19. Do you have usability and user experience (UX) teams in OB design and development projects?
20. Do you conduct usability/UX evaluations of OB systems before roll out to clients?
21. Does your bank belong to any banking consortium, local or international?
22. Do SA banks collaborate with third parties (e.g. information security practitioners) to improve OB and the general banking security environment?
23. Do SA banks share ideas among themselves on general security-related problems to aid system development and improve their offerings?
24. What are the advantages and disadvantages of legacy IT infrastructures and processes to the deployment of OB services?
25. How scalable are legacy IT infrastructures in offering OB services?

Section D: Online banking policy and regulations

26. Do you have a dedicated OB information security policy or terms and conditions (Ts&Cs) that are separate from the general banking service?
27. Do the terms and conditions cover access of client information to third parties?
28. Which legislation governs the provision of OB between clients and banks in SA?
29. Which legislation governs the protection of personal information of clients held by banks in SA?
30. Are SA banks compelled to report any security breaches to a governing body?
31. Do you communicate dispute resolution channels to clients for OB-related problems?
32. In terms of dispute resolution, is there a separate system for clients to lodge OB related disputes?

Section E: User training and awareness

33. Does the bank have online fraud/threats awareness campaigns for clients?
34. Does the bank provide channels to report any suspicious activities for online banking users?
35. Where can the client get more information on OB fraud prevention?
36. Does the bank have a fraud reporting system for clients?
37. Does the bank communicate responsibilities and liabilities associated with the use of OB to clients?
38. Are there any specific challenges the bank face in improving the end-to-end security of clients' computers and the bank systems?
39. Does the bank provide assistance to clients to improve the end-to-end security of the communication channel?
40. Do you have any suggestions on how users can alter their behaviour/actions to create a more secure OB environment?

THANK YOU FOR YOUR PARTICIPATION!

Appendix G: Survey responses sample

Please tick the check box o	A1. Gender:	A2. Age:	A3. Home language (Pleas	A4. Highest educational qu	A5. Employment status:
I accept	1	3	1	5	1
I accept	2	4	1	4	1
I accept	1	2	2	4	1
I accept	1	1	1	5	1
I accept	1	5	1	5	2
I accept	1	5	1	5	2
I accept	1	5	1	3	1
I accept	1	5	1	4	4
I accept	1	5	1	5	1
I accept	2	1	10	1	3
I accept	2	3	10	5	1
I accept	2	2	3	4	1
I accept	2	2	10	4	1
I accept	1	5	1	2	2
I accept	1	3	10	5	1
I accept	1	3	10	5	1
I accept	1	2	1	4	1
I accept	1	4	1	2	1
I accept	1	5	1	4	2
I accept	1	3	10	5	1
I accept	2	3	10	5	1
I accept	2	3	3	5	1
I accept	1	3	10	5	1
I accept	1	3	1	5	1
I accept	1	3	10	5	1
I accept	2	3	10	5	1
I accept	2	2	3	5	1
I accept	1	3	4	5	1
I accept	1	4	1	5	1
I accept	1	2	1	5	1

A6. Income per month bef	A7. South African province	A8. Ethnic group:	B9. Please choose ONLY	B10. How long have you b	B11. How often do you us e
6	3	1	3	3	1
3	3	2	1	5	2
2	9	2	3	4	1
4	9	3	5	4	3
6	3	2	1	5	1
6	3	2	1	5	1
3	4	2	6	5	1
3	9	2	6	5	2
4	9	2	6	5	3
1	1	1	1	1	1
4	3	1	6	5	2
1	3	1	6	3	1
1	3	1	6	1	4
2	9	2	3	4	1
4	8	1	6	5	1
4	3	1	6	3	1
2	9	3	2	4	1
1	9	2	2	2	4
6	3	2	1	5	1
3	3	1	2	2	3
4	1	1	3	4	2
2	4	1	6	5	2
4	4	1	6	5	2
3	4	1	3	4	2
3	1	1	6	5	1
3	4	1	6	5	1
3	3	1	3	4	1
6	3	1	3	2	3
5	2	1	6	4	4
4	3	1	1	3	2
3	3	1	5	3	2
4	3	1	3	2	2

B12. Which device(s)	Computer (at work)	Public computer (internet cafe)	Laptop/portable device	Mobile device	Other	a. I find online banking use
1	0	0	1	1	0	5
1	0	0	1	1	0	5
1	0	0	1	1	0	5
1	1	0	1	1	0	5
1	1	0	1	1	0	5
1	1	0	1	1	0	5
0	0	0	1	0	0	5
1	0	0	1	1	0	5
1	1	0	0	1	0	5
1	0	0	0	0	0	3
1	0	0	0	0	0	5
0	0	0	0	1	0	5
0	1	0	0	0	0	5
1	1	0	1	1	0	5
1	1	0	1	1	0	4
0	0	0	1	0	0	4
1	1	0	1	1	0	5
1	0	0	0	1	0	4
0	1	0	0	0	0	5
0	1	0	1	1	0	5
1	1	0	0	0	0	5
1	0	0	1	1	0	5
1	1	0	1	1	0	5
1	0	0	0	1	0	5
1	0	0	1	1	0	5
1	1	0	1	1	0	5
0	1	0	1	1	0	5
1	1	0	0	0	0	5
1	1	0	1	1	0	5
0	1	0	0	1	0	5
0	0	0	1	0	0	5

b. Using online banking he	c. Using online banking in	d. Online banking saves m	e. Online banking does ev	f. I find online banking eas	g. It is easy for me to beco
5	5	5	2	4	5
5	5	5	4	5	5
4	5	5	3	5	4
5	5	5	4	5	5
5	5	5	4	5	5
5	5	5	4	5	5
5	5	5	3	4	5
5	5	5	4	5	5
5	3	5	4	4	5
4	4	4	2	3	3
5	5	5	4	5	4
5	5	5	4	5	3
5	5	5	5	5	4
5	5	5	4	4	4
5	5	5	1	5	4
5	5	5	3	2	3
5	4	4	5	4	5
5	4	4	4	4	4
5	5	5	3	4	4
4	3	5	3	5	4
5	5	5	5	4	4
5	4	4	3	4	4
5	2	4	2	5	4
5	5	5	3	4	5
5	5	5	4	5	5
5	5	5	4	5	5
5	5	5	5	4	4
5	5	5	4	5	4
5	5	5	3	4	5

Appendix H: Complete list of frequencies

Table H-1: Frequencies (*n*=540)

Factor	Category	Frequency	Percentage	Cumulative percentage
Gender	Male	314	58.1	58.1
	Female	226	41.9	100.0
Age	Below 20 years	26	4.8	4.8
	20-29 years	122	22.6	27.4
	30-39 years	195	36.1	63.5
	40-49 years	88	16.3	79.8
	Above 50 years	109	20.2	100.0
Language	English	241	44.6	44.6
	Afrikaans	117	21.7	66.3
	Zulu	57	10.6	76.9
	Sotho	34	6.3	83.2
	Xhosa	33	6.1	89.3
	Venda	5	0.9	90.2
	Tsonga	5	0.9	91.1
	Swazi	3	0.6	91.6
	Ndebele	8	1.5	93.1
	Other	37	6.9	100.0
Education	No formal education	3	0.6	0.6
	Matric	58	10.7	11.3
	Post-matric certificate/diploma	124	23.0	34.3
	Degree	104	19.3	53.5
	Postgraduate degree	239	44.3	97.8
	Other	12	2.2	100.0
Employment	Employed	431	79.8	79.8
	Self-employed	53	9.8	89.6
	Unemployed	28	5.2	94.8
	Retired	14	2.6	97.4
	Other	14	2.6	100.0
Income	Less than R10 000	73	13.5	13.5
	R10 000-R19 999	68	12.6	26.1
	R20 000-R29 999	102	18.9	45.0
	R30 000-R39 999	130	24.1	69.1
	R40 000-R49 999	46	8.5	77.6
	R50 000 or more	121	22.4	100.0
Province	Eastern Cape	44	8.1	8.1
	Free State	25	4.6	12.8
	Gauteng	250	46.3	59.1
	KwaZulu-Natal	59	10.9	70.0
	Limpopo	8	1.5	71.5
	Mpumalanga	3	0.6	72.0
	North West	5	0.9	73.0
	Northern Cape	7	1.3	74.3
	Western Cape	139	25.7	100.0

Factor	Category	Frequency	Percentage	Cumulative percentage
Ethnicity	Black	198	36.7	36.7
	White	234	43.3	36.7
	Coloured	23	4.3	80.0
	Indian/Asian	85	15.7	84.3
Bank	Absa	90	16.7	100.0
	Capitec	53	9.8	16.7
	FNB	162	30.0	26.5
	Investec	12	2.2	56.5
	Nedbank	83	15.4	58.7
	Standard Bank	140	25.9	74.1
Experience	Below 1 year	39	7.2	100.0
	1-2 years	46	8.5	15.7
	3-4 years	96	17.8	33.5
	5-6 years	97	18.0	51.5
	7 years and above	262	48.5	100.0
Use frequency	Every day	185	34.3	34.3
	Once a week	214	39.6	73.9
	Once in two weeks	71	13.2	87.1
	Once a month	65	12.0	99.1
	Other	5	0.9	100.0
Device	Mobile	398	73.7	
	PC	390	72.2	
	Laptop	331	61.3	
Device combinations	Any 1 device	134	24.8	24.8
	2 or more devices	406	75.2	100.0

Appendix I: SEM measurement models

This appendix provide figures and tables for each SEM measurement model referred to in chapter 5 section 5.7.1.

Table of figures

List of tables

I1. Testing of PE model

The measurement model of the latent variable performance expectancy (PE) consists of five observable variables – PEa, PEb, PEc, PEd, and PEe – that are measured by means of a five-point Likert scale. The model is represented in Figure I-1.

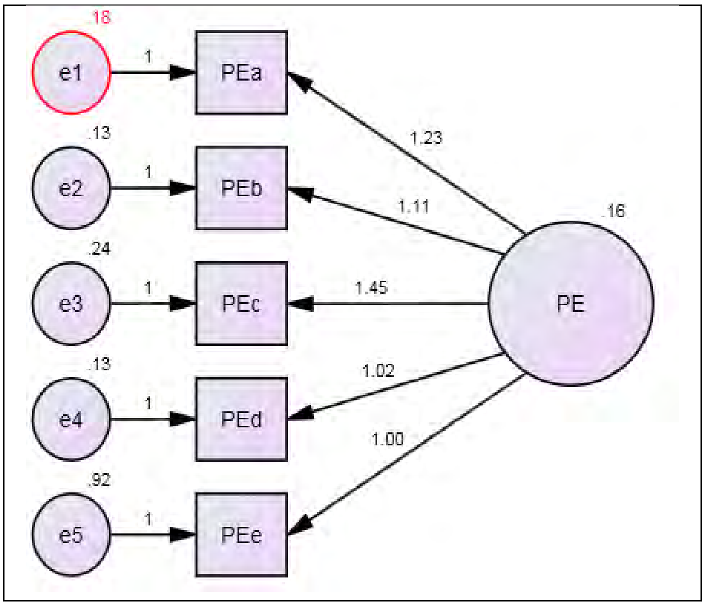


Figure I-1: Measurement model of PE

Table I-1 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-1: Model fit indices of PE measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	41.848	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	8.370		
CFI		0.961	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.117	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.016	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.969	GFI ≥ 0.90	Above the threshold; this shows good fit

The results of Table I-1 show that the fit indices CFI, SRMR, and GFI were the only indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2 and RMSEA). Taken together, the fit indices indicated that the model was not a good fit and needed improvement. In order to modify the measurement model so that it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. Table I-2 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters.

Table I-2: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e3 <--> e4	14.585
e5 <--> e4	7.555

After treating e3 and e4, as well as e5 and e4, as free parameters, the measurement model was rerun. Figure I-2 shows the modified model.

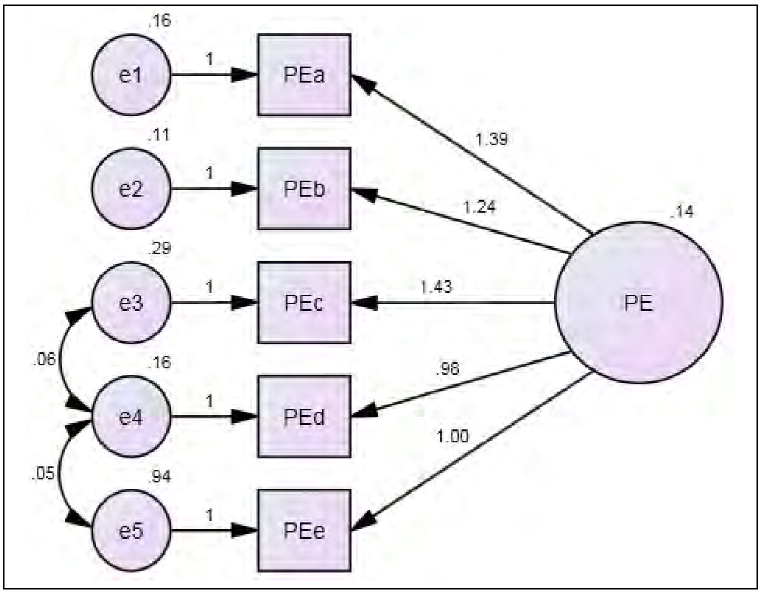


Figure I-2: Modified PE model

Table I-3 shows the extracted fit indices, with all indices, taken together, showing a good model fit.

Table I-3: Model fit indices of PE modified model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	8.450	Ratio $2.1 \leq (\chi^2/\text{df}) \leq 3.1$	χ^2/df is within the range; this indicates that the model shows good fit
	df	3		
	χ^2/df	2.817		
CFI		0.994	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.058	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.011	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.994	GFI ≥ 0.90	Above the threshold; this shows good fit

I2. Testing of EE model

The measurement model of the latent variable effort expectancy (EE) consists of six observable variables – EEa, EEb, EEc, EEd, EEe, and EEf – that are measured by means of a five-point Likert scale. The model is represented in Figure I-3.

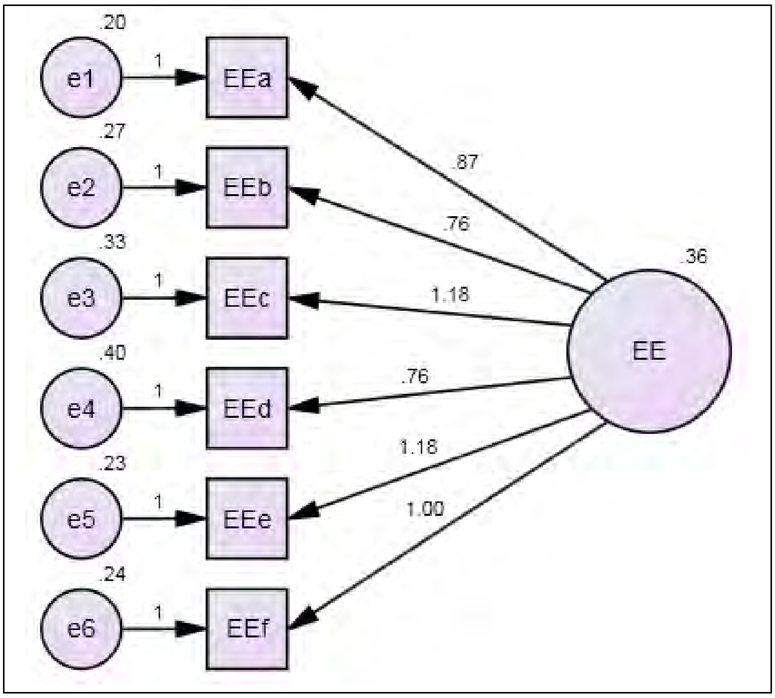


Figure I-3: Measurement model of EE

Table I-4 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-4: Model fit indices of EE measurement model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	65.550	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	9		
	χ^2/df	7.283		
CFI		0.962	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.108	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.019	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.961	GFI ≥ 0.90	Above the threshold; this shows good fit

The results of Table I-4 show that the fit indices CFI, SRMR, and GFI were the only indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2 and RMSEA). Even though more than half of the fitness test showed a good fit, a better model could be achieved by modifying the models that suggested modification. In order to modify the measurement model, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. Table I-5 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters.

Table I-5: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e2 <--> e1	27.973
e6 <--> e4	5.210
e6 <--> e1	5.014
e4 <--> e3	4.098

After treating the identified pairs of residual covariances as free parameters, the measurement model was rerun, and Figure I-4 shows the modified model.

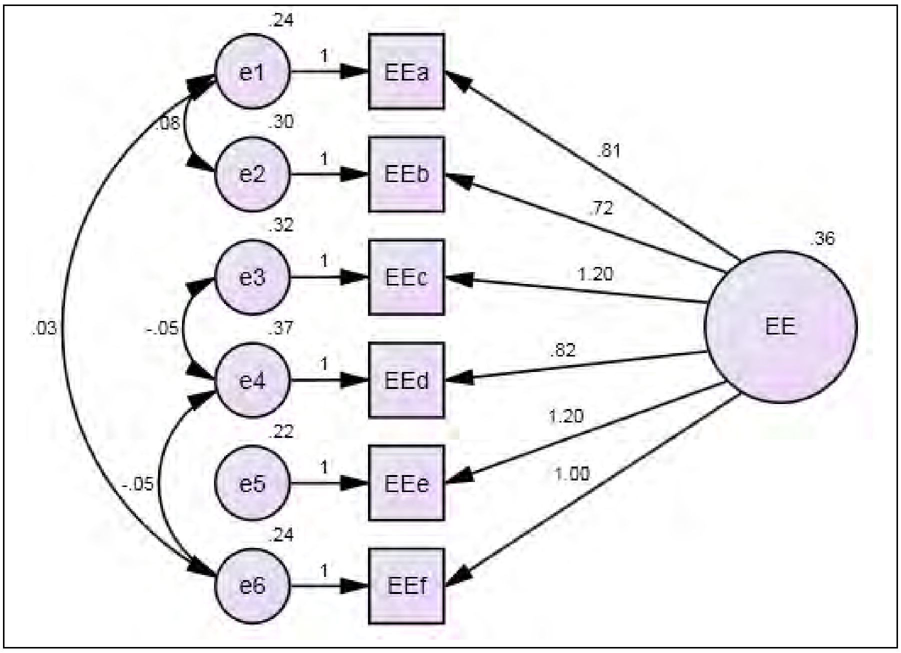


Figure I-4: Modified EE model

Table I-6 shows the extracted fit indices, and all indices show a good model fit. Taken together, the fit indices indicate a good model fit.

Table I-6: Model fit indices of EE modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	14.889	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	5		
	χ^2/df	2.978		
CFI		0.993	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.061	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.010	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.991	GFI ≥ 0.90	Above the threshold; this shows good fit

I3. Testing of SI model

The measurement model of the latent variable social influence (SI) consists of four observable variables – SIa, SIb, SIc, and SId – that are measured by means of a five-point Likert scale. The model is represented in Figure I-5.

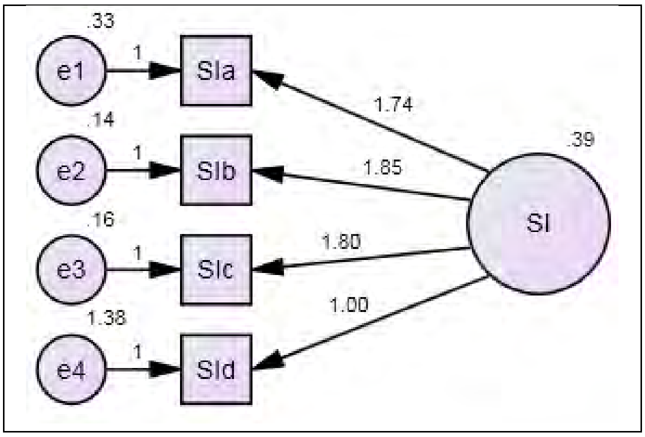


Figure I-5: Measurement model of SI

Table I-7 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-7: Model fit indices of SI measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	12.832	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	2		
	χ^2/df	6.416		
CFI		0.994	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.100	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.025	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.989	GFI ≥ 0.90	Above the threshold; this shows good fit

The results of Table I-7 show that the fit indices CFI, SRMR, and GFI were the only indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2 and RMSEA). Taken together, the fit indices indicate that the model is not a good fit and needs improvement.

In order to modify the measurement model, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. After treating the identified residual covariance pairs that had the highest modification indices as free parameters, the model became poorer than it had been before modification; therefore, the research reverted to the original model. The results of the original model can be accepted, as three out of five indices showed good fit.

I4. Testing of FC model

The measurement model of the latent variable facilitating conditions (FC) consists of four observable variables – FCa, FCb, FCc, and FCd – that are measured by means of a five-point Likert scale. The model is represented in Figure I-6.

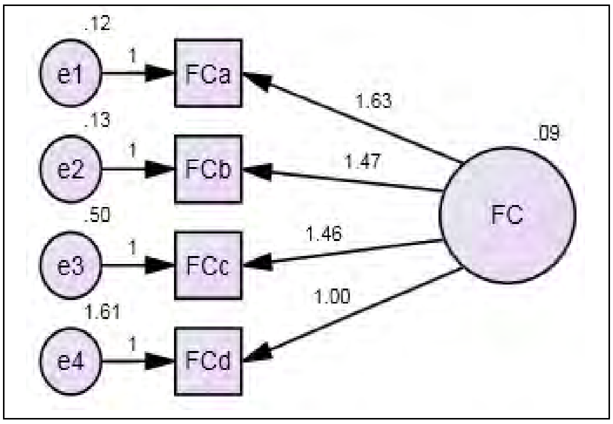


Figure I-6: Measurement model of FC

Table I-8 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-8: Model fit indices of FC measurement model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	33.628	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	2		
	χ^2/df	16.814		
CFI		0.931	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.171	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.064	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.971	GFI ≥ 0.90	Above the threshold; this shows good fit

The results of Table I-8 show that the SRMR and GFI were the only fit indices that showed good fit of the model, while model modification would be recommended for the rest of the fit indices (χ^2, CFI, and RMSEA). Taken together, the fit indices indicate that the model is not a good fit and needs improvement. In order to modify the measurement model, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters. Table I-9 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters.

Table I-9: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e4 <--> e3	29.095

After treating the modification indices in Table I-13 as free parameters, the measurement model was rerun, and Figure I-7 shows the modified model.

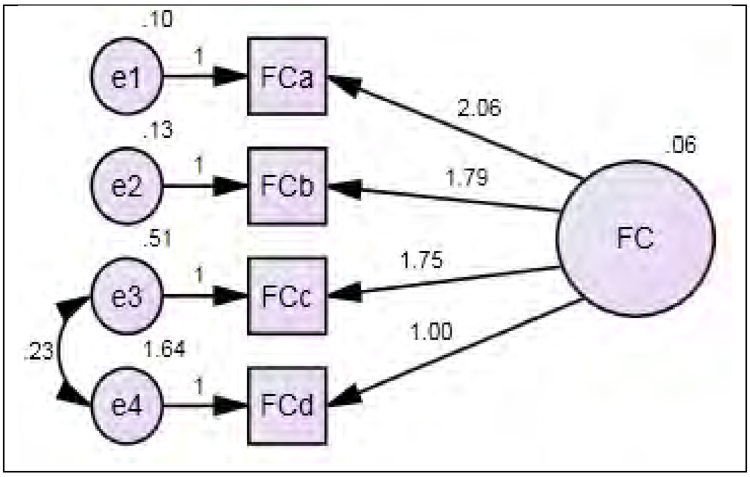


Figure I-7: Modified FC model

Table I-10 shows the extracted fit indices, and all indices show a good model fit. Taken together, the fit indices indicate a good model fit.

Table I-10: Model fit indices of FC modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	2.943	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	1		
	χ^2/df	2.943		
CFI		0.996	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.060	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.010	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.997	GFI ≥ 0.90	Above the threshold; this shows good fit

I5. Testing of HM model

The measurement model of the latent variable hedonic motivation (HM) consists of four observable variables – HMa, HMb, HMc, and HMd – that are measured by means of a five-point Likert scale. The model is represented in Figure I-8.

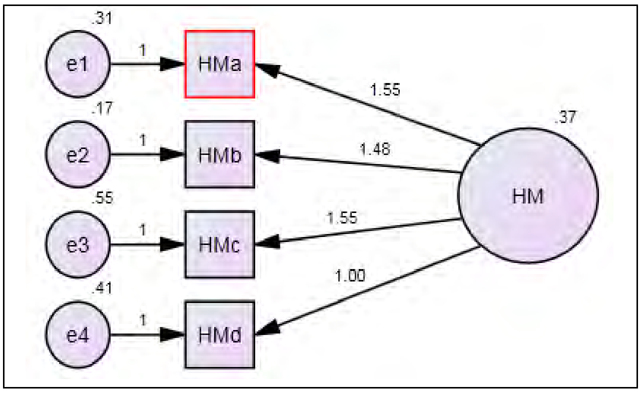


Figure I-8: Measurement model of HM

Table I-11 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-11: Model fit indices of HM measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	21.703	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	2		
	χ^2/df	10.852		
CFI		0.984	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.135	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.022	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.981	GFI ≥ 0.90	Above the threshold; this shows good fit

The results of Table I-11 show that three out of five indices showed good fit, while two indices suggested model modification. CFI, SRMR, and GFI were the indices that showed good fit, while χ^2 and RMSEA suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-12: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e4 <--> e1	12.392

Table I-12 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure 9 shows the modified model.

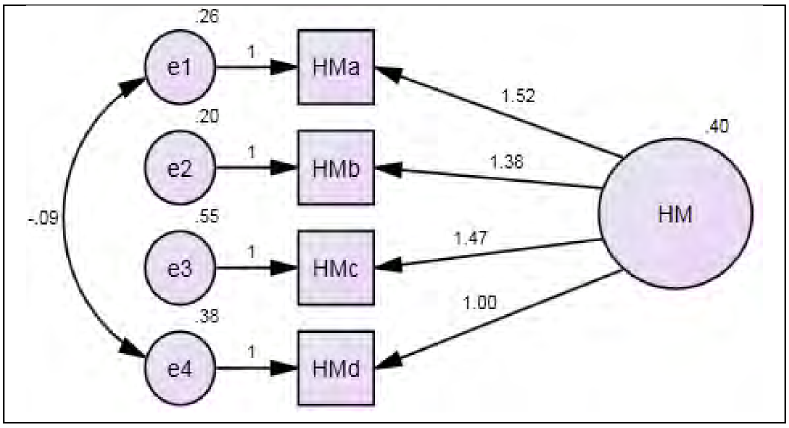


Figure I-9: Modified HM model

Table I-13 shows the extracted fit indices, and all indices show a good model fit. Taken together, the fit indices indicate a good model fit.

Table I-13: Model fit indices of HM modified model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	2.837	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	1		
	χ^2/df	2.837		
CFI		0.999	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.058	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.010	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.997	GFI ≥ 0.90	Above the threshold; this shows good fit

I6. Testing of PV model

The measurement model of the latent variable price value (PV) consists of three observable variables – PVa, PVb, and PVc – that are measured by means of a five-point Likert scale. The model is represented in Figure I-10.

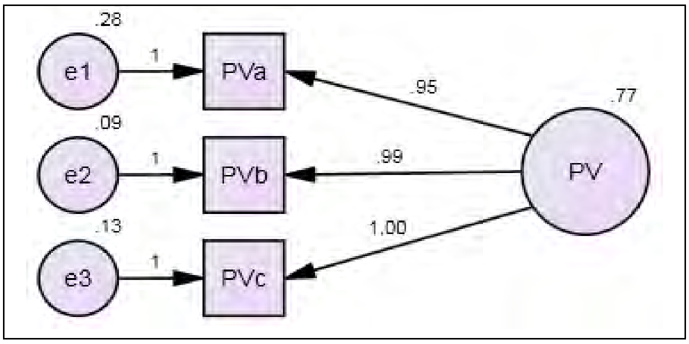


Figure I-10: Measurement model of PV

Table I-14 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-14: Model fit indices of PV measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	0.00	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is undefined; df is 0, meaning that there are no degrees of freedom
	df	0		
	χ^2/df	Undefined		
CFI		1.000	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.914	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.000	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		1.000	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-14 show that only two models had a good fit, that is, SRMR and GFI; the rest suggested model modification. The χ^2 value showed degrees of freedom of zero. According to (Kline 2015), when the degrees of freedom are zero, that means that there is no way to affirm or reject the model; it means that the data have no 'freedom' to vary, and there is no 'freedom' to conduct research with this data set. Therefore, this measurement model will not be used in the structural model.

I7. Testing of H model

The measurement model of the latent variable habit (H) consists of five observable variables – Ha, Hb, Hc, Hd, and He – that are measured by means of a five-point Likert scale. The model is represented in Figure I-11.

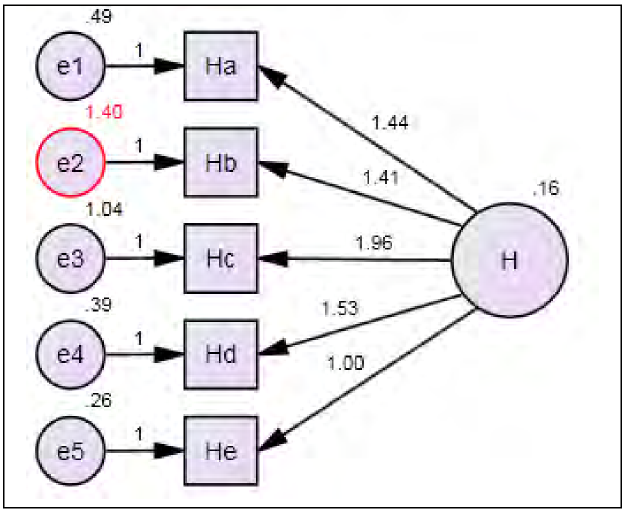


Figure I-11: Measurement model of H

Table I-15 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-15: Model fit indices of H measurement model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	200.127	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	40.025		
CFI		0.717	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.269	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.153	RMR ≤ 0.08	Above the threshold value; this shows that the model needs modification
GFI		0.869	GFI ≥ 0.90	Below the threshold; this shows that the model needs modification

The results of Table I-15 show that none of the fit indices showed a good fit – hence, suggesting modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-16: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e3 <--> e2	133.074
e2 <--> e1	10.229
e5 <--> e3	11.366

Table I-16 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-12 shows the modified model.

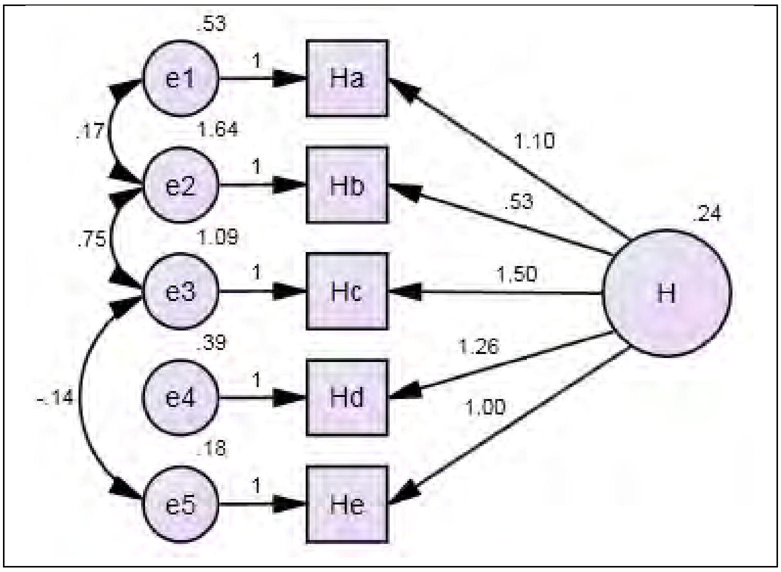


Figure I-12: Modified H model

Table I-17 shows the extracted fit indices, and all indices show a good model fit. Taken together, the fit indices indicate a good model fit.

Table I-17: Model fit indices of H modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	5.644	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	2		
	χ^2/df	2.822		
CFI		0.995	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.058	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.022	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.996	GFI ≥ 0.90	Above the threshold; this shows good fit

I8. Testing of BI model

The measurement model of the latent variable behavioural intention (BI) consists of three observable variables – BIa, Bib, and BIc – that are measured by means of a five-point Likert scale. The model is represented in Figure I-13.

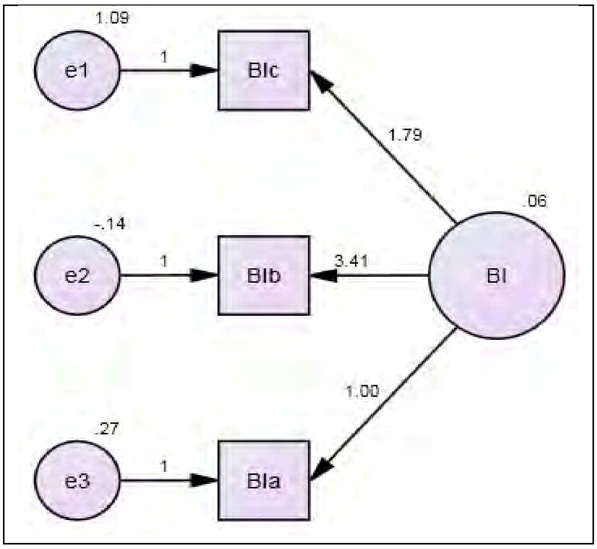


Figure I-13: Measurement model of BI

Table I-18 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-18: Model fit indices of BI measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	0.000	Ratio 2.1 ≤ χ^2/df) ≤ 3.1	χ^2/df is undefined; df is 0, meaning that there are no degrees of freedom
	df	0		
	χ^2/df	Undefined		
CFI		1.000	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.401	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.000	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		1.000	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-18 show that three models had a good fit, that is, CFI, SRMR, and GFI, while the other two suggested model modification. The χ^2 value showed degrees of freedom of zero. As mentioned earlier, when the degrees of freedom are zero that means that there is no way to affirm or reject the model (Kline 2015). It means that the data have no 'freedom' to vary and that there is no 'freedom' to conduct research with this data set. However, because the construct BI is a mediator of several variables from the original UTAUT model, this model cannot be rejected; therefore, the research will use it as is in the structural model.

I9. Testing of UL model

The measurement model of the latent variable usability – learnability (UL) consists of five observable variables – ULa, ULb, ULc, ULd, and ULe – that are measured by means of a five-point Likert scale. The model is represented in Figure I-14.

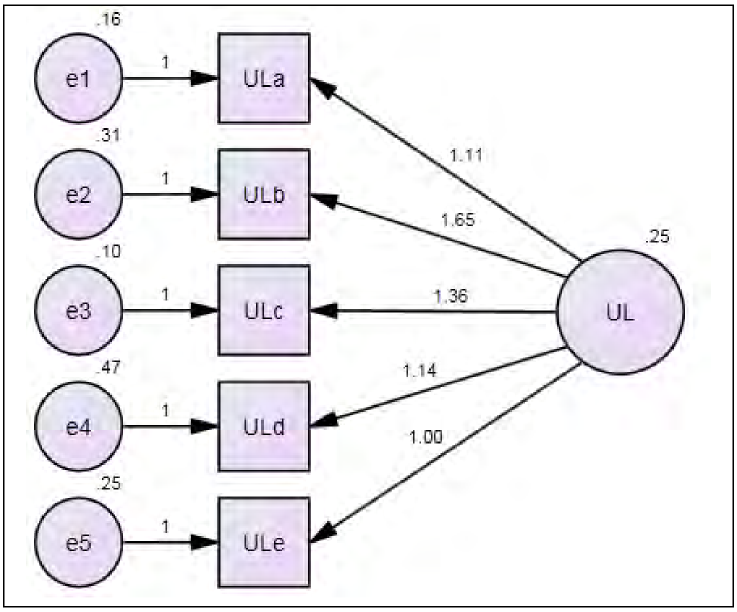


Figure I-14: Measurement model of UL

Table I-19 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-19: Model fit indices of UL measurement model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	107.779	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	21.556		
CFI		0.934	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.195	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.036	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		0.929	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-19 show that two fit indices – SRMR and GFI – out of the five measure-fit indices showed a good fit. Three of the fit indices, namely, CFI, RMSEA, and χ^2, suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-20: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e5 <--> e4	88.323
e4 <--> e2	4.247

Table I-20 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-15 shows the modified model.

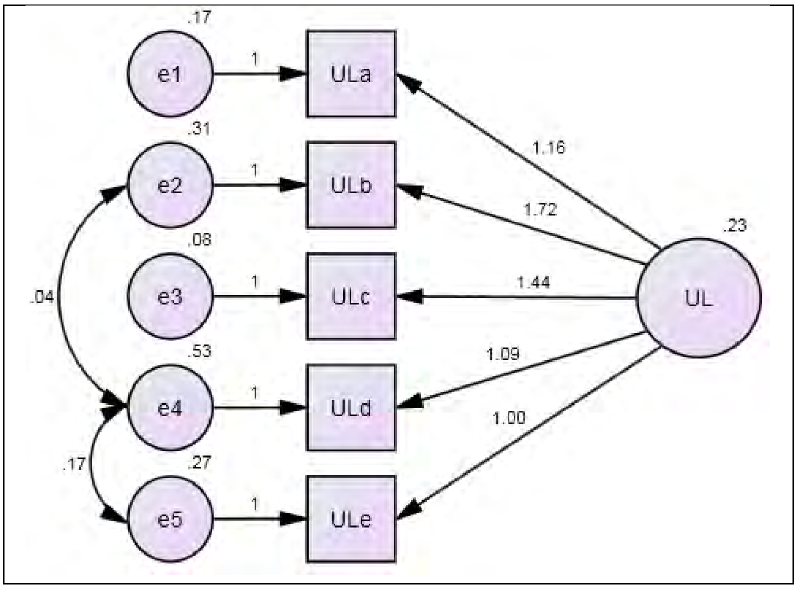


Figure I-15: Modified UL model

Table I-21 shows the extracted fit indices, and all indices show a good model fit. Taken together, the fit indices indicate a good model fit.

Table I-21: Model fit indices of UL modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	7.897	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	3		
	χ^2/df	2.632		
CFI		0.997	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.055	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.009	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.994	GFI ≥ 0.90	Above the threshold; this shows good fit

I10. Testing of UUS model

The measurement model of the latent variable usability – user satisfaction (UUS) consists of three observable variables – UUSa, UUSb, and UUSc – that are measured by means of a five-point Likert scale. The model is represented in Figure I-16.

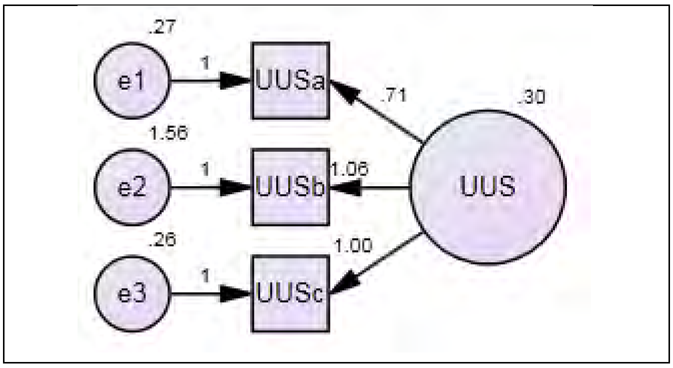


Figure I-16: Measurement model of UUS

Table I-22 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-22: Model fit indices of UUS measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	0.00	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is undefined; df is 0, meaning that there are no degrees of freedom
	df	0		
	χ^2/df	Undefined		
CFI		1.000	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.331	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.000	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		1.000	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-22 show that only two models had a good fit, that is, SRMR and GFI; the rest suggested model modification. The χ^2 value showed degrees of freedom of zero. When the degrees of freedom are zero that means there is no way to affirm or reject the model. Therefore, the measurement model for US will not be used in the structural model.

I11. Testing of US model

The measurement model of the latent variable usability – satisfaction (US) consists of five observable variables – USa, USb, USc, USd, and USe – that are measured by means of a five-point Likert scale. The model is represented in Figure I-17.

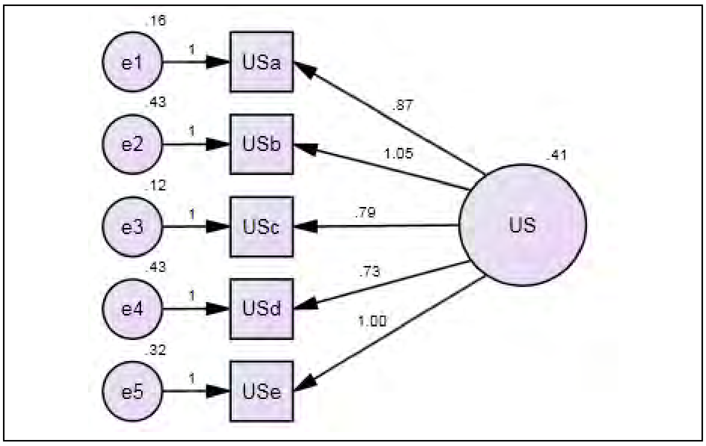


Figure I-17: Measurement model of US

Table I-23 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-23: Model fit indices of US measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	67.289	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	13.458		
CFI		0.948	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.152	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.032	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		0.951	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-23 show that two fit indices – SRMR and GFI – out of the five measure-fit indices showed a good fit. Three of the fit indices, CFI, RMSEA, and χ^2, suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-24: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e5 <--> e4	29.494
e4 <--> e2	8.972
e4 <--> e1	11.603

Table I-24 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-18 shows the modified model.

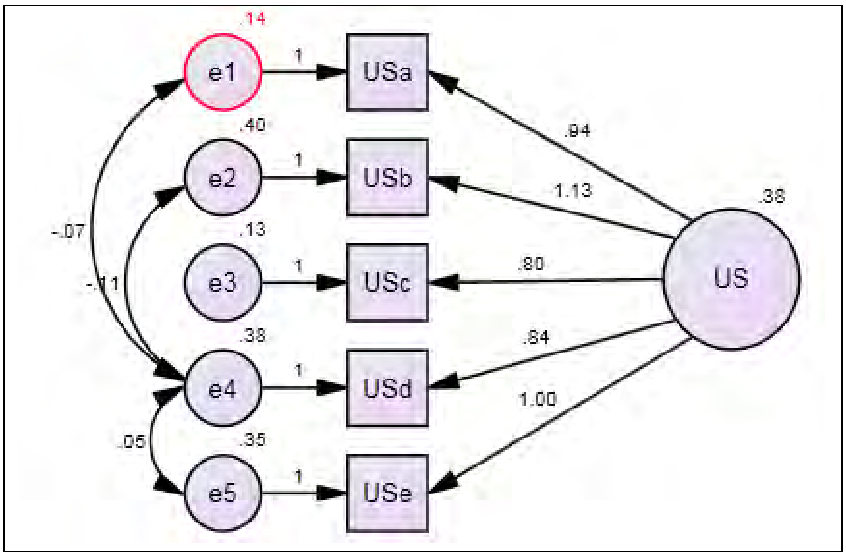


Figure I-18: Modified US model

Table I-25 shows the extracted fit indices. Four out five indices showed a good model fit. RMSEA was the only model fit that was slightly below the minimum of the threshold required. On the one hand, considering the complexity of SEM, achieving four models of fitness out of the five required is acceptable; hence, no further modification was done. On the other hand, further modification might result in other model fit indices such as χ^2 again falling out of range.

Table I-25: Model fit indices of US modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	4.385	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	2		
	χ^2/df	2.193		
CFI		0.998	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.047	0.05 ≤ (RMSEA) ≤ 0.080	Slightly below the minimum required; this shows that it needs modification
SRMR		0.007	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.997	GFI ≥ 0.90	Above the threshold; this shows good fit

I12. Testing of UA model

The measurement model of the latent variable usability – availability (UA) consists of five observable variables – UAa, UAb, UAc, UAd, and UAe – that are measured by means of a five-point Likert scale. The model is represented in Figure I-19.

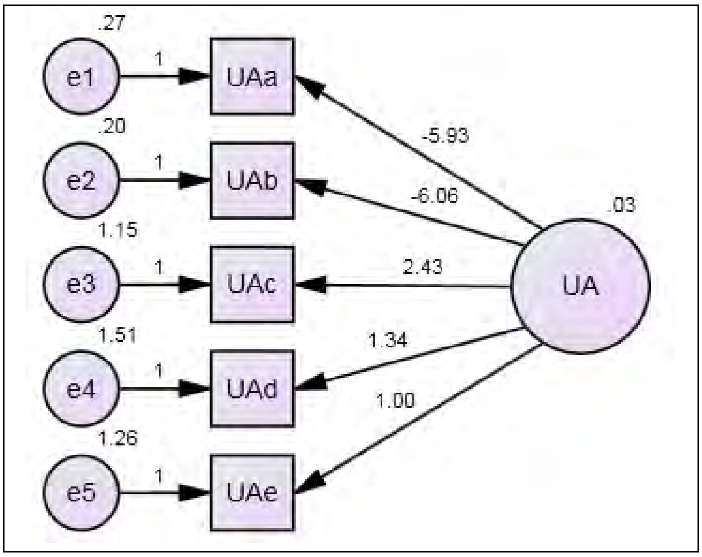


Figure I-19: Measurement model of UA

Table I-30 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-26: Model fit indices of UA measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	78.125	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	15.625		
CFI		0.896	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.165	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.133	RMR ≤ 0.08	Above the threshold value; this shows that the model needs modification
GFI		0.940	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-30 show that only GFI out of the five measure-fit indices showed a good fit. Four of the fit indices, namely, CFI, SRMR, RMSEA, and χ^2, suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-27: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e5 <--> e3	27.699
e4 <--> e3	29.827

Table I-27 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-20 shows the modified model.

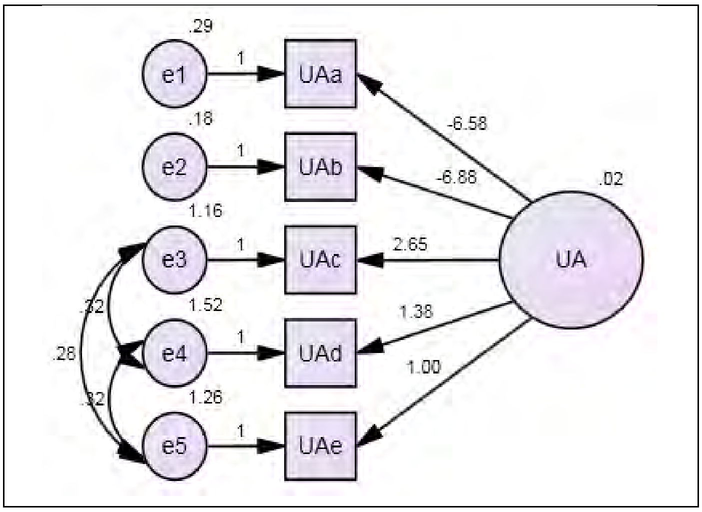


Figure I-20: Modified UA model

Table I-28 shows the extracted fit indices. Three out five indices showed a good model fit. RMSEA and χ^2 were the two model fit indices that were out of range – hence, suggesting further modification. Further modification resulted in an unidentifiable model; therefore, the research settled for the maximum fit that could be obtained, as shown in Figure I-20. It is important to note that, after accepting such model fit, when the measurement models are put together to form the structural model, if the structural model does not fit and requires further modification by deleting some constructs or construct items, then measurement models such as that of UA will be the first to consider for deletion.

Table I-28: Model fit indices of UA modified model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	0.53	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is below the minimum threshold; this indicates that the model needs further modification
	df	2		
	χ^2/df	0.027		
CFI		1.000	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.000	0.05 ≤ (RMSEA) ≤ 0.080	Below the minimum threshold, this shows that the model needs modification
SRMR		0.001	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		1.000	GFI ≥ 0.90	Above the threshold; this shows good fit

I13. Testing of UE model

The measurement model of the latent variable usability – errors (UE) consists of five observable variables – UEa, UEb, UEc, UEd, and UEe – that are measured by means of a five-point Likert scale. The model is represented in Figure I-21.

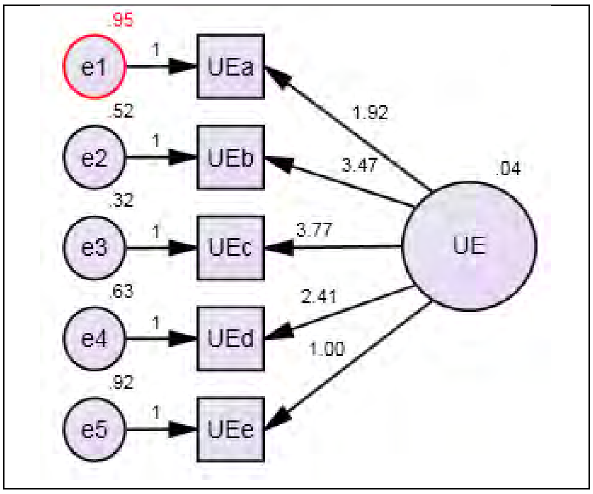


Figure I-21: Measurement model of UE

Table I-29 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-29: Model fit indices of UE measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	52.869	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	10.574		
CFI		0.890	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.133	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.056	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		0.961	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-29 show that GFI and SRMR out of the five measure-fit indices showed a good fit. The CFI, RMSEA, and χ^2 fit indices suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-30: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e2 <--> e1	19.287
e5 <--> e4	13.913
e5 <--> e2	15.789

Table I-30 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-22 shows the modified model.

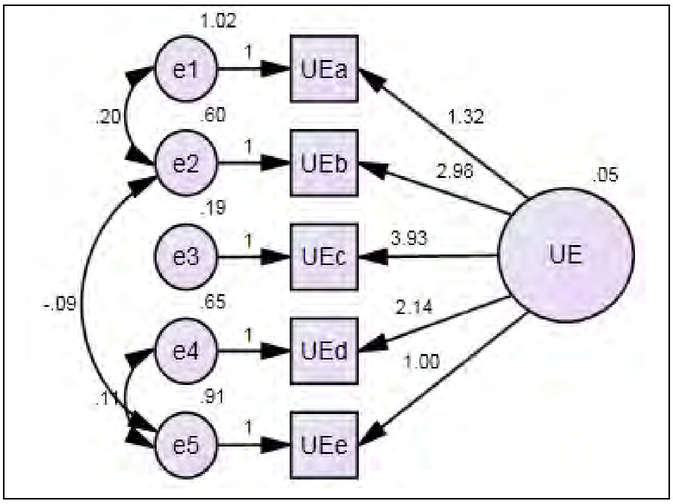


Figure I-22: Modified UE model

Table I-31 shows the extracted fit indices. Four out five indices showed a good model fit. Only RMSEA suggested model modification. However, when the measurement model of RMSEA is rounded off to the nearest two decimal places, as it is in the threshold, its value becomes 0.05, which is equal to the minimum of the RMSEA threshold; hence, the RMSEA was accepted as showing good fit.

Table I-31: Model fit indices of UE modified model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	4.576	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	2		
	χ^2/df	2.288		
CFI		0.994	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.049	0.05 ≤ (RMSEA) ≤ 0.080	Equal to the minimum threshold when rounded off to two decimal places; hence, the model is a slightly good fit
SRMR		0.018	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.997	GFI ≥ 0.90	Above the threshold; this shows good fit

I14. Testing of UHD model

The measurement model of the latent variable usability help and documentation (UHD) consists of six observable variables – UHDa, UHDb, UHDc, UHDd, UHDe, and UHDf – that are measured by means of a five-point Likert scale. The model is represented in Figure I-23.

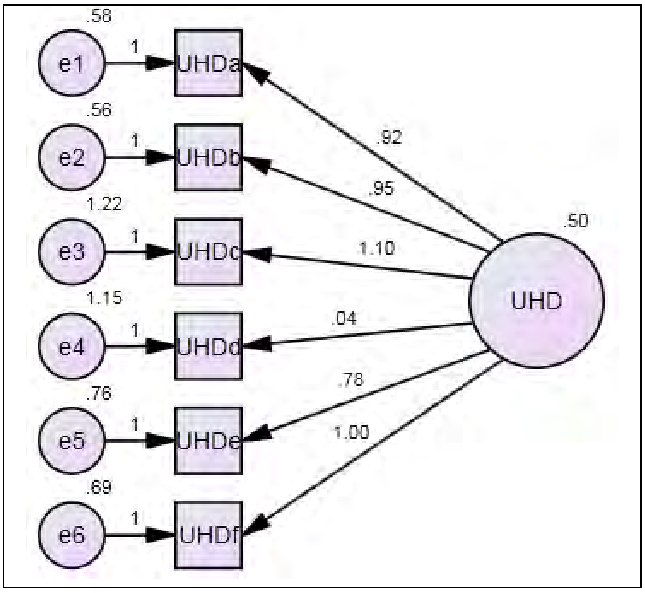


Figure I-23: Measurement model of UHD

Table I-32 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-32: Model fit indices of UHD measurement model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	69.503	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	9		
	χ^2/df	7.723		
CFI		0.898	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.112	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.071	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		0.956	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-32 show that GFI and SRMR out of the five measure-fit indices showed a good fit. The CFI, RMSEA, and χ^2 fit indices suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-33: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e6 <--> e4	19.287
e4 <--> e3	13.913
e6 <--> e2	15.789

Table I-33 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-24 shows the modified model.

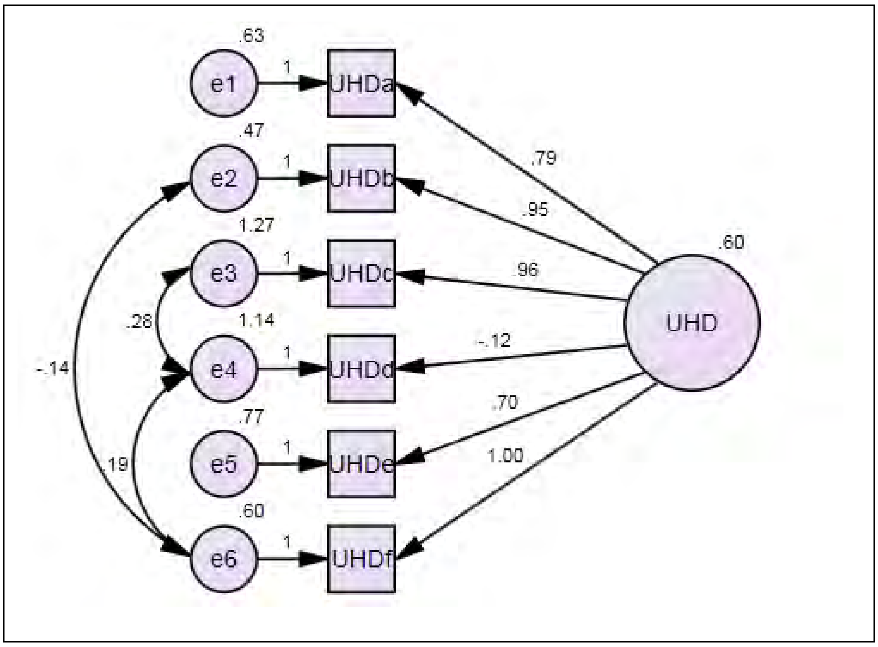


Figure I-24: Modified UHD model

Table I-34 shows the extracted fit indices. Four out of five indices showed a good model fit, with the exception of χ^2, which suggested model modification. Modifying the model for χ^2 could result in both χ^2 and RMSEA not fitting. Therefore, in order to achieve maximum fit, the research accepted the modified model, as shown in Figure I-24.

Table I-34: Model fit indices of UHD modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	26.175	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	6		
	χ^2/df	4.362		
CFI		0.966	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.079	0.05 ≤ (RMSEA) ≤ 0.080	Equal to the minimum threshold when rounded off to two decimal places; hence, the model is a slightly good fit
SRMR		0.036	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.985	GFI ≥ 0.90	Above the threshold; this shows good fit

I15. Testing of S model

The measurement model of the latent variable security (S) consists of five observable variables – Sa, Se, Sf, Sg, and Sm – that are measured by means of a five-point Likert scale. The model is represented in Figure I-25.

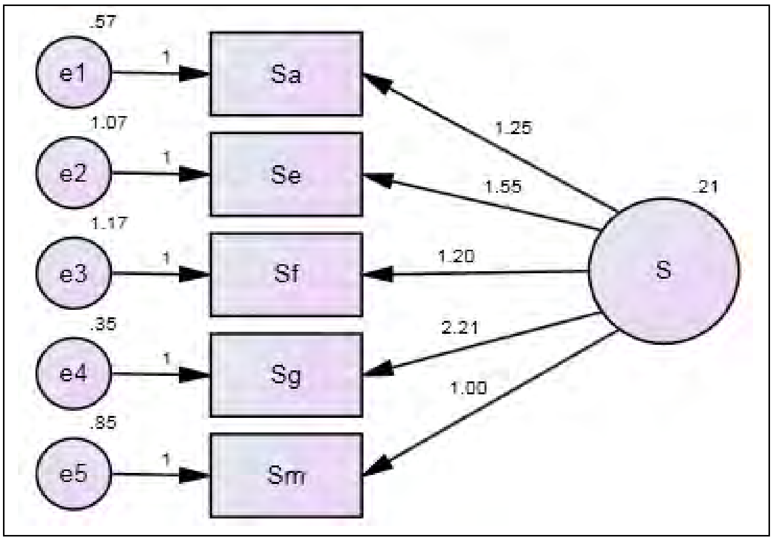


Figure I-25: Measurement model of S

Table I-35 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-35: Model fit indices of S measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	35.552	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	5		
	χ^2/df	7.110		
CFI		0.943	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.106	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.067	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		0.974	GFI ≥ 0.90	Above the threshold; this shows that the model has good fit

The results of Table I-35 show that GFI and SRMR out of the five measure-fit indices showed a good fit. Three of the fit indices, CFI, RMSEA, and χ^2, suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-36: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e3 <--> e2	23.359

Table I-36 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-26 shows the modified model.

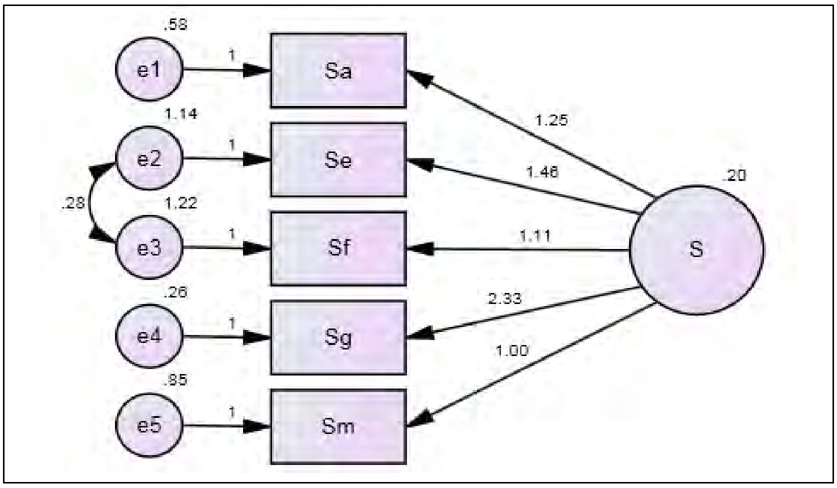


Figure I-26: Modified S model

Table I-37 shows that all the extracted fit indices showed a good model fit.

Table I-37: Model fit indices of S modified model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	9.837	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	4		
	χ^2/df	2.459		
CFI		0.989	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.052	0.05 ≤ (RMSEA) ≤ 0.080	Equal to the minimum threshold when rounded off to two decimal places; hence, the model is a slightly good fit
SRMR		0.026	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.993	GFI ≥ 0.90	Above the threshold; this shows good fit

I16. Testing of P model

The measurement model of the latent variable privacy (P) consists of seven observable variables – Pb, Pc, Pd, Ph, Pi, Pj, and Pk – that are measured by means of a five-point Likert scale. The model is represented in Figure I-27.

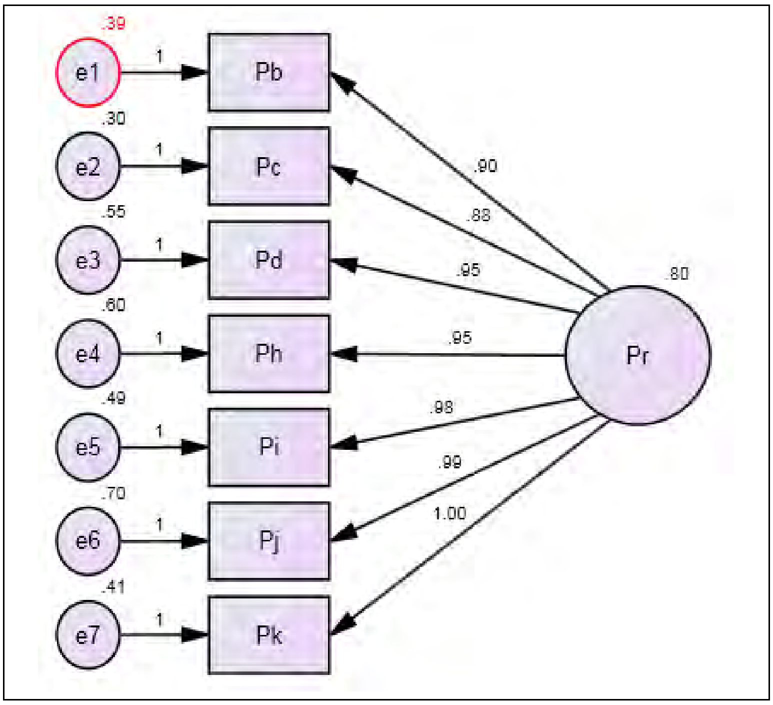


Figure I-27: Measurement model of P

Table I-38 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-38: Model fit indices of P measurement model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	343.524	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	14		
	χ^2/df	24.537		
CFI		0.868	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.209	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.076	RMR ≤ 0.08	Below the threshold value; this shows that the model has good fit
GFI		0.830	GFI ≥ 0.90	Below the threshold; this shows that the model needs modification

The results of Table I-38 show that only SRMR out of the five measure-fit indices showed a good fit. Four of the fit indices, GFI, CFI, RMSEA, and χ^2, suggested model modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-39: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e6 <--> e5	96.118
e2 <--> e1	91.605
e3 <--> e2	60.852
e6 <--> e2	47.591
e7 <--> e6	42.326
e3 <--> e1	14.702

Table I-39 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-28 shows the modified model.

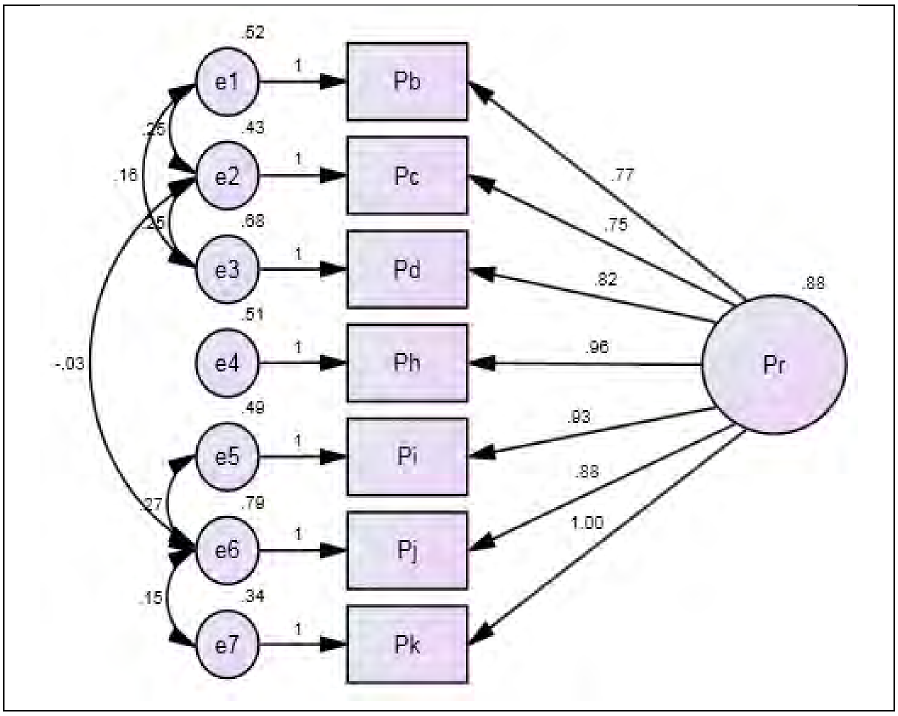


Figure I-28: Modified P model

Table I-40 shows that all the extracted fit indices showed a good model fit.

Table I-40: Model fit indices of P modified model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	19.204	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	8		
	χ^2/df	2.401		
CFI		0.996	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.051	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; hence, the model is a good fit
SRMR		0.020	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.990	GFI ≥ 0.90	Above the threshold; this shows good fit

I17. Testing of SUS model

The measurement model of the system usability scale (SUS) consists of 10 observable variables – SUSa, SUSb, SUSc, SUSd, SUSe, SUSf, SUSg, SUSh, SUSi, and SUSj. The latent variable SUS is measured by means of the 10 observable variables with a five-point Likert scale. The model is represented in Figure I-29.

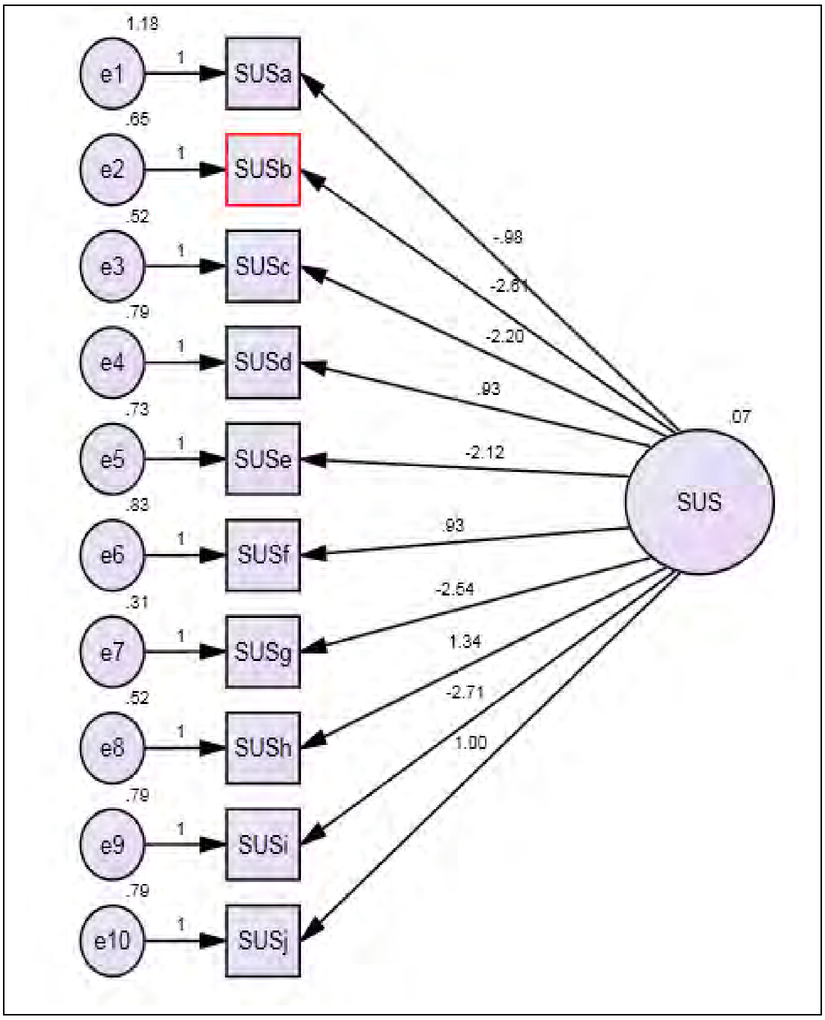


Figure I-28: Measurement model of SUS

Table I-41 demonstrates the extracted results from Amos output of the measurements of the fit indices compared to their thresholds.

Table I-41: Model fit indices of SUS measurement model

Fit indices		Measurement model	Threshold	Recommendations for the measurement model
Chi-squared	χ^2	506.622	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is too large and out of the range of the threshold; this indicates that the model needs modification
	df	35		
	χ^2/df	14.475		
CFI		0.656	CFI ≥ 0.950	Below the threshold; this shows that the model needs modification
RMSEA		0.158	0.05 ≤ (RMSEA) ≤ 0.080	Above the threshold; this suggests that the model needs modification
SRMR		0.109	RMR ≤ 0.08	Above the threshold value; this shows that the model needs modification
GFI		0.812	GFI ≥ 0.90	Below the threshold; this shows that the model needs modification

The results of Table I-42 show that none of the fit indices showed a good fit – hence, suggesting modification. In order to modify the measurement model so it could fit, pairs of residual covariances that had the highest modification indices were identified and treated as free parameters.

Table I-42: Extract of modification indices of covariances from Amos output

Error terms	Modification index covariance
e10 <--> e8	93.738
e6 <--> e4	67.894
e4 <--> e1	31.161
e8 <--> e6	26.936
e10 <--> e6	41.175
e7 <--> e2	26.848
e9 <--> e1	20.305
e10 <--> e4	13.033
e8 <--> e4	17.753
e5 <--> e4	11.822

Table I-42 shows the identified residual covariance pairs that had the highest modification indices that needed to be treated as free parameters. After treating the identified modification indices as free parameters, the measurement model was rerun, and Figure I-30 shows the modified model.

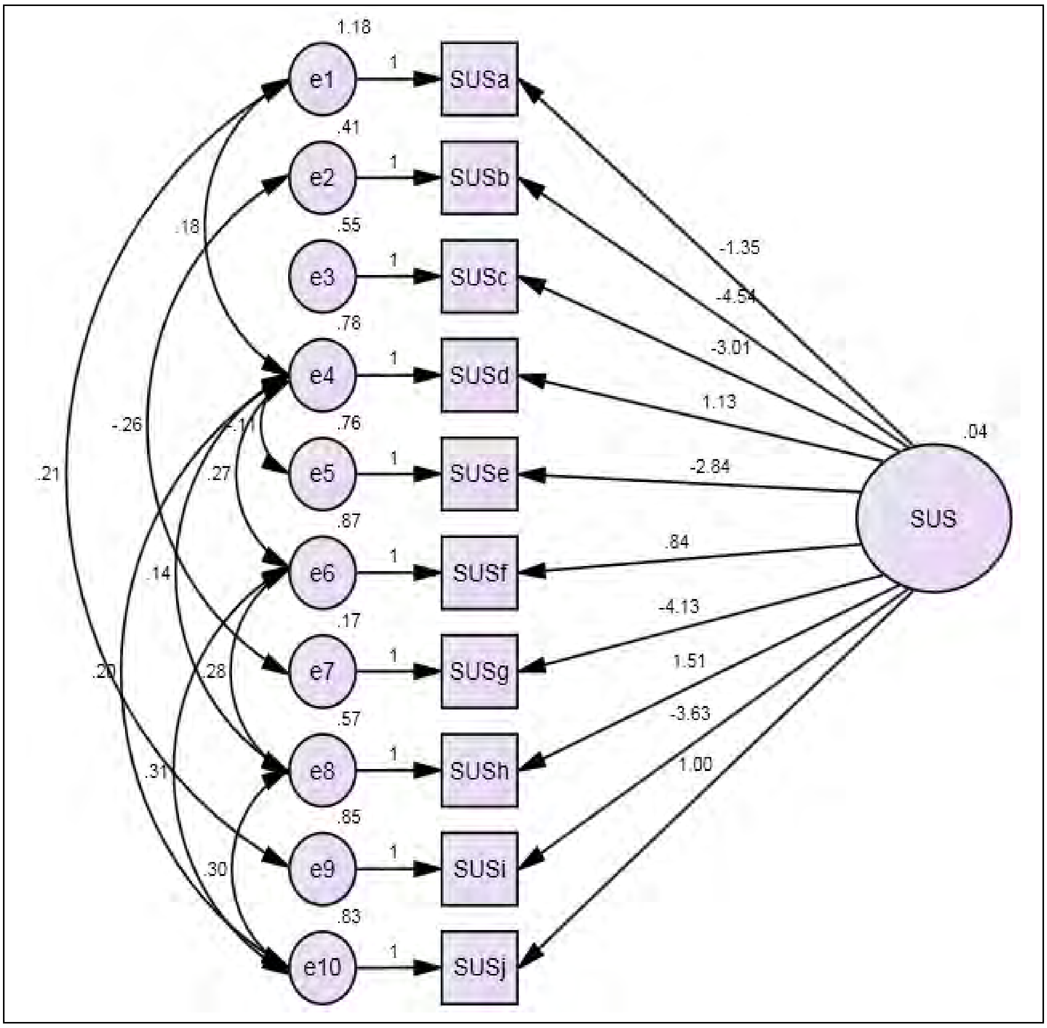


Figure I-30: Modified SUS model

Table I-43 shows the extracted fit indices, and all indices show a good model fit. Taken together, the fit indices indicate a good model fit.

Table I-43: Model fit indices of SUS modified model

Fit indices		**Measurement model**	**Threshold**	**Recommendations for the measurement model**
Chi-squared	χ^2	74.535	Ratio 2.1 ≤ (χ^2/df) ≤ 3.1	χ^2/df is within the range; this indicates that the model shows good fit
	df	25		
	χ^2/df	2.981		
CFI		0.964	CFI ≥ 0.950	Above the threshold; this shows good fit
RMSEA		0.061	0.05 ≤ (RMSEA) ≤ 0.080	Within the range; this shows good fit
SRMR		0.045	RMR ≤ 0.08	Below the threshold value; this shows good fit
GFI		0.973	GFI ≥ 0.90	Above the threshold; this shows good fit

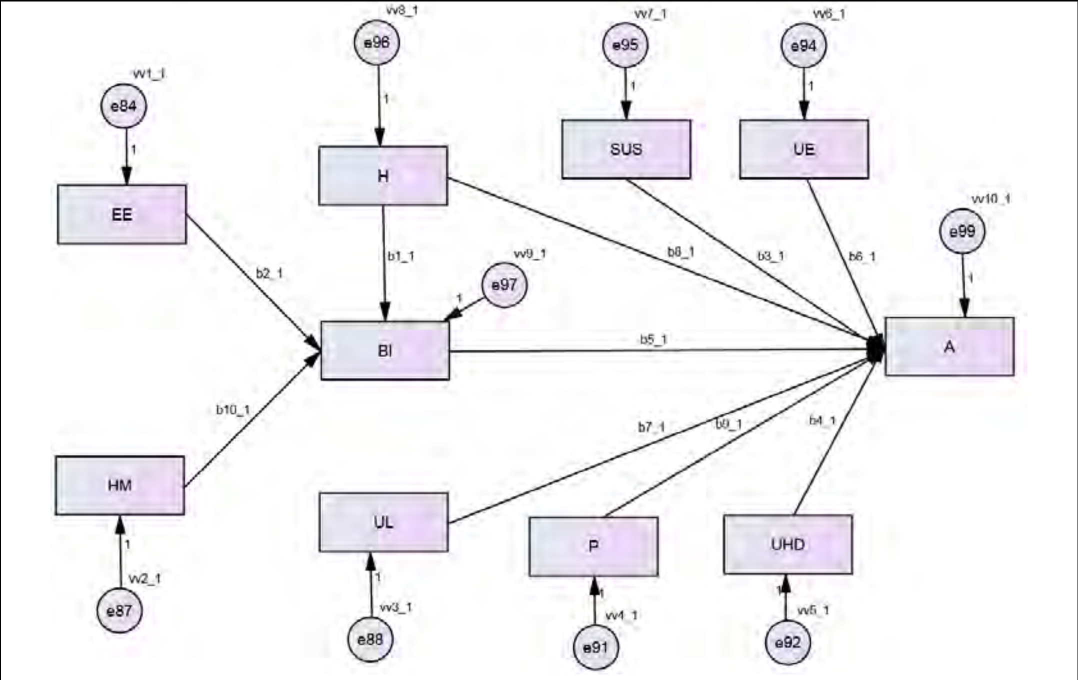
Appendix J: SEM integrated model

This appendix presents the integrated SEM model and analysis of moderating factors.

Table J-1: Dichotomous recoding of moderator variables

#	Variable	Original coding	New coding
1	Gender	1 = Male 2 = Female	Used as is
2	Age	1 = Below 20 years 2 = 20-29 years 3 = 30-39 years 4 = 40-49 years 5 = Above 50 years	1 = Below 30 years (1-2) 2 = 30 and above years (3-5)
3	Experience	1 = Below 1 year 2 = 1-2 years 3 = 3-4 years 4 = 5-6 years 5 = Above 7 years	1 = 4 years and below 2 = Above 4 years
4	Education	1 = No formal education 2 = Matric 3 = Post-matric/diploma 4 = Degree 5 = Postgraduate degree 6 = Other	1 = No tertiary education (1-2) 2 = Tertiary education (3-6)
5	Employment	1 = Employed 2 = Self-employed 3 = Unemployed 4 = Retired 5 = Other	1 = Employed (1-2) 2 = Not employed (3-5)
6	Ethnicity	1 = Black 2 = White 3 = Coloured 4 = Indian/Asian	1 = Black (1) 2 = Non-black (2-4)
7	Devices	1 = One device 2 = More than one device	Used as is
8	Income	1 = Less than R10 000 2 = R10 000-R19 999 3 = R20 000-R29 999 4 = R30 000-R39 999 5 = R40 000-R49 999 6 = R50 000 or more	1 = Less than R30 000 (1-3) 2 = R30 000 or more (3-6)
9	Use frequency	1 = Every day 2 = Once a week 3 = Once every two weeks 4 = Once a month 5 = Other	1 = Daily (1) 2 = All other (2-5)

Group 1 (b2_1)



Group 2 (b2_2)

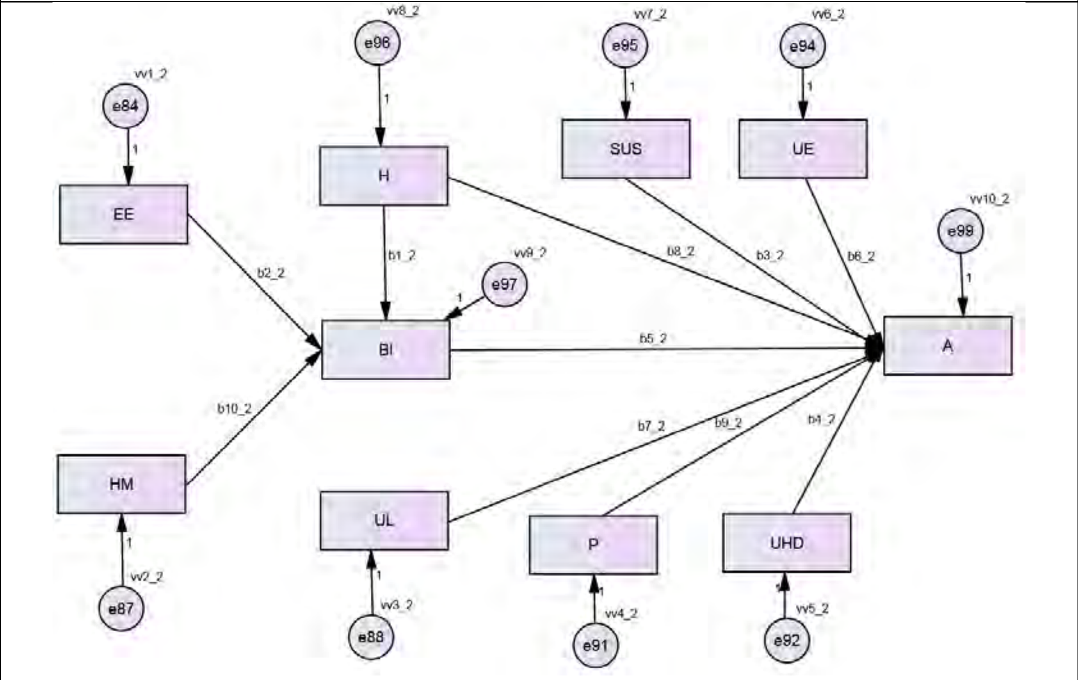


Figure J-1: Dichotomous models

Table J-2: Chi-squared difference test and regression weights

Moderator	Relationship	Model number	DF	CMIN	P	Hypothesis result	Regression weight	Meaning of hypothesis result
Gender	Model level	Chi-squared test	10	24.061	0.007	Supported		The p-value was below 0.05, meaning that the groups were different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	3.752	0.53	Not supported		Multigroup analysis showed that there was no difference between gender groups; hence, gender did not moderate the relationship between hedonic motivation (HM) and behavioural intention (BI).
	BI ← H	Chi-squared test	1	1.513	0.474	Not supported		Multigroup analysis showed that there was no difference between gender groups; hence, gender did not moderate the relationship between BI and habit (H).
	Adoption ← H	Chi-squared test	1	0.569	0.451	Not supported		Multigroup analysis showed that there was no difference between gender groups; hence, gender did not moderate the relationship between adoption and H.
Age	Model level	Chi-squared test	10	18.285	0.050	Supported		The p-value was equal to 0.05, meaning that the groups were different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	0.066	0.798	Not supported		Multigroup analysis showed that there was no difference among age groups; hence, age did not moderate the relationship between BI and HM.
	BI ← H	Chi-squared test	1	1.120	0.290	Not supported		Multigroup analysis showed that there was no difference among age groups; hence, age did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	2.273	0.132	Not supported		Multigroup analysis showed that there was no difference among age groups; hence, age did not moderate the relationship between adoption and H.

Experience	Model level	Chi-squared test	10	20.625	.024	Supported		The p-value was less than 0.05, meaning that the groups were different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	1.483	0.223	Not supported		Multigroup analysis showed that there was no difference between experience groups; hence, experience did not moderate the relationship between BI and HM.
	BI ← H	Chi-squared test	1	0.000	0.993	Not supported		Multigroup analysis showed that there was no difference between experience groups; hence, experience did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	6.367	0.012	Supported		Multigroup analysis showed that there was a difference between experience groups; hence, experience moderated the relationship between adoption and H.
		Less experienced					0.24	The moderating effects of experience on the relationship between adoption and H were greater for less experienced participants than the more experienced.
		More experienced					0.17	
Education	Model level	Chi-squared test	10	15.847	0.104	Not supported		The p-value was above 0.05, meaning that the groups were not different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	0.317	0.573	Not supported		Multigroup analysis showed that there was no difference among education levels; hence, education level did not moderate the relationship between BI and HM.
	BI ← H	Chi-squared test	1	0.189	0.664	Not supported		Multigroup analysis showed that there was no difference among education levels; hence, education level did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	0.281	0.596	Not supported		Multigroup analysis showed that there was no difference among education levels; hence, education level did not moderate the relationship between adoption and H.

Employment	Model level	Chi-squared test	10	19.181	0.038	Supported		The p-value was below 0.05, meaning that the groups were different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	1.419	0.234	Not supported		Multigroup analysis showed that there was no difference among employment levels; hence, employment did not moderate the relationship between BI and HM.
	BI ← H	Chi-squared test	1	0.910	0.340	Not supported		Multigroup analysis showed that there was no difference among employment levels; hence, employment did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	2.258	0.133	Not supported		Multigroup analysis showed that there was no difference among employment levels; hence, employment did not moderate the relationship between adoption and H.
Ethnicity	Model level	Chi-squared test	10	23.384	0.009	Supported		The p-value was below 0.05, meaning that the groups were different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	6.521	0.011	Supported		Multigroup analysis showed that there was a difference between ethnicity groups; hence, ethnicity moderated the relationship between BI and HM.
		African					0.21	The moderating effects of ethnicity on the relationship between BI and HM were greater for the non-African race than the African race.
		Non-African					0.28	
	BI ← H	Chi-squared test	1	0.093	0.760	Not supported		Multigroup analysis showed that there was no difference among ethnicity groups; hence, ethnicity did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	5.198	0.023	Supported		Multigroup analysis showed that there was a difference among ethnicity groups; hence, ethnicity moderated the relationship between adoption and H.
		African					0.14	

		Non-African					0.15	The moderating effects of ethnicity on the relationship between adoption and H were greater for the non-African race than the African race.
Devices	Model level	Chi-squared test	10	15.869	0.103	Not supported		The p-value was above 0.05, meaning that the groups were not different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	0.045	0.831	Not supported		Multigroup analysis showed that there was no difference between participants who used one devices to access internet banking and those who used two or more devices; hence, the number of devices did not moderate the relationship between BI and HM.
	BI ← H	Chi-squared test	1	0.828	0.363	Not supported		Multigroup analysis showed that there was no difference between participants who used one devices to access internet banking and those who used two or more devices; hence, the number of devices did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	1.693	0.193	Not supported		Multigroup analysis showed that there was no difference between participants who used one devices to access internet banking and those who used two or more devices; hence, the number of devices did not moderate the relationship between adoption and H.
Income	Model level	Chi-squared test	10	25.564	0.004	Supported		The p-value was less than 0.05, meaning that the groups were different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	4.208	0.040	Supported		Multigroup analysis showed that there was a difference between low-income earners and high-income earners when it came to the relationship between adoption and H; hence, income moderated the relationship between adoption and H.
		Below R30 000					0.283	The moderating effects of income on the relationship between BI and HM were greater for individuals who earned R30 000 per month or more than for those who earned less than R30 000.
		Above R30 000					0.315	

	BI ← H	Chi-squared test	1	0.037	0.847	Not supported		Multigroup analysis showed that there was no difference between participants who earned less than R30 000 and those who earned above R30 000. Therefore, income did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	0.059	0.807	Not supported		Multigroup analysis showed that there was no difference between participants who earned less than R30 000 and those who earned above R30 000. Therefore, income did not moderate the relationship between adoption and H.
Use frequency	Model level	Chi-squared test	10	17.085	0.073	Not supported		The p-value was above 0.05, meaning that the groups were not different at model level. Further investigation needs to be done for different hypothesised relationships.
	BI ← HM	Chi-squared test	1	1.185	0.276	Not supported		Multigroup analysis showed that there was no difference between daily users of online banking and all other users. Therefore, use frequency did not moderate the relationship between BI and HM.
	BI ← H	Chi-squared test	1	3.084	0.079	Not supported		Multigroup analysis showed that there was no difference between daily users of online banking and all other users. Therefore, use frequency did not moderate the relationship between BI and H.
	Adoption ← H	Chi-squared test	1	0.023	0.878	Not supported		Multigroup analysis showed that there was no difference between daily users of online banking and all other users. Therefore, use frequency did not moderate the relationship between adoption and H.

Appendix K: Interview transcript sample

NOTE: The interviews were transcribed verbatim from the audio recordings, and no (spoken) grammar errors were fixed.

Researcher (R): Are there are any training for what are the responsibilities?

Participant (P): So, the customer we don’t give a formal or set of training documentation or offer that they can come for training. We do not do that. But we do put certain statements on the system where they can like questions and answers (FAQ) type of thing, which can help them with certain things. But we don’t go out to the customer and help him to use his system properly. In the retail space it’s a bit difficult if you have 6.5 million customers to offer training so we do offer guidelines but not formal training.

R: What if a specific person or customer need specifically or ask for something?

P: So, if a customer call, okay lets I think one of your questions was, do we have a process for handling customer queries or controls or questions around online banking? We do have call centre where they can call into. Uhm so when they call into the call centre they deal with all queries but there’s one specific line you go to if you have an internet banking or online banking query. You will then be reverted to a desk probably that is technical that can help you with either the technical issues or explain to you how it works.

R: To go about?

P: How the thing go, if you want make a payment how the thing will work if you want to if a see an error code, what it actually means and you don’t understand and also if you need advice on security they will give that as well. So, we have a dedicated call centre for all those and all calls are recorded and tracked and feedback is given to the customer that way, so technical and non-technical.

R: So, the call centre is it 24 hour or office hours?

P: I think uhm I think it’s not a fully 24 hour unless you have a fraud query. It is fraud query that’s 24/7 so if you have a fraud issue on your online banking. And let’s say your online banking has been compromised, that’s 24/7 you can call immediately it will be blocked so that you cannot be, if they are phishing you, you can be certain you can block immediately and no further phishing attempts would be ava... well we would actually try to track them and close them down. So, does that answer your question?

R: Yeah it does and are there any client reports any specific challenges on the different channels?

P: So the clients do have various options on complaining, so first of all those who use internet banking has a specific place where they can complain. Although they can complain another over another normal channels, like a call centre or branch or anywhere they want to complain because all our contact areas with customers they can complain on any of those. Even on the app that we have or the internet banking site itself, there's an area where they can actually communicate to us or complain.

R: So, in terms of that feedback, are there any form or channels, which the users can actually request those like, is it like by writing you an email is it sufficient groups?

P: So, there are, even on the app there is a communications area within the app where its' secure although slow. But they can also send us an email, and then they can also go through our call centre there is a specific call centre number. But most people use the, use a email as communication, majority of them. Because the people at the branch may get it and may have no idea of what the guy is saying and then you don't get the idea.

R: What are the incentives put in place to encourage digital banking?

P: No charges, yeah, I think majority of the banks have no charges for digital. So there, but I do not know of any charges. You don't pay to sign up, you don't pay a monthly fee it's usually included all your products in bundles.

R: Yeah you mentioned the terms and conditions, you provide them besides are there incentives to make sure?

P: So there are several awareness campaigns either in branches or at business sometimes at, if there are small business forums for example we may have thing, get them to say be aware of the following scams, phishing whatever and look out for the following, it will be good if you install Trustier and we will rehash the awareness around what the terms and conditions are as well. So, we definitely have, i want to ongoing campaigns of various natures to actually inform customers of their roles, their responsibilities. As well as the dangers that goes with sharing of passwords, opening emails with attachments, malware so we do have a lot of communication and awareness that goes with that and various channels, not just.

R: Yes, because I was asking in respect before this Cyber bill that is coming, that were their gaps in the current copy of the electronic communication act?

P: Yeah, I think the gaps are more in the implementation practical implementation side. Also, I think, I'm not sure if the legislative capability to legislate for new technology at this moment. I think there's definitely gaps. For example, cyber has a big issue with things like block chain, yet it is a very good method to protect your information. Use the hash and things to protect integrity. But they have no understanding of it and now they say you can't do that because of the bitcoin link. But if they really know how it works they would probably say it's a very good technology to use. So, I think the gaps are that there's a lack of understanding of knowledge in the regulator perspective on how this technology actually work and how it is, what are the risks related to that. And then they don't know what to or how to legislate stuff. I just think that the regulator also haven't made the connection to say that but if you take mobile, if you take digital, if you take cyber, they actually all inter linked. And if you looked at the legislative communications area they really effective. I mean and then if you look at the banking legislation they very effective. So, they don't have that over all coordinated view so I think the gaps are very much still there. Yeah so I don't think they are 100% effective or efficient to actually legislate what is required. I mean even the legal side, if there are legal issues related to cyber I don't know if our legal environment has enough people who understand IT and Law, especially IT I don't know many advocates that can do that.

R: And you mentioned SABRIC? Is there a, is it just a coming together?

P: SABRIC is a formal association of all the South African banks, or any banks in South Africa.

R: Is it compulsory for any bank in South Africa?

P: Yeah, I think, I don't think you have to be a member but most of the banks are. SABRIC is the basically I can't tell you exact acronym stands for. It stands for South African banking something against crime, it's there to actually prevent fraud and crime. Criminal activities against banks and their customers.

Appendix L: Framework evaluation tool

SECTION A: Introduction

My name is Mathias Mujinga, and I am doing a PhD study at UNISA under the supervision of Prof MM Eloff (Research Professor: Institute for Corporate Citizenship) and Prof JH Kroeze (Professor: School of Computing). I invite you to participate in this framework evaluation process. The purpose of this evaluation tool is to validate the proposed socio-technical information security (STInfoSec) framework for the design of secure and usable online information security applications.

The framework is part of a PhD study entitled “A Socio-Technical Framework for Secure and Usable Online Information Security Systems”. The framework is specifically designed for online banking service as a case study, but is intended to be applicable to other general online information security applications, with appropriate adaptations tailored to those applications. The principles provided here for evaluation were first selected from previous studies in literature, then based on survey and interview findings from online banking users and banking personnel, respectively, the list has been refined in the context of online banking service. Checklist items for each principle were developed into this preliminary framework.

As an evaluator, you are requested to rate the importance of each of the proposed design principles and their respective checklist items with regard to their relevance in addressing security- and usability-related problems of the service. Specifically, these principles are envisaged to assist the design and, ultimately, improve the service. Your participation in this study is highly appreciated.

Please kindly complete and submit the evaluation survey to the researcher as soon as possible. The evaluation tool will take at most approximately 60 minutes to complete.

SECTION B: Consent form

Please note that by submitting this form, you agree that you have not been put under any pressure to participate in this evaluation exercise and are willingly participating in it. Also, please note that participation is voluntary and that you may withdraw at any time without negative consequences. Please understand that your answers to these questions will be used for academic purposes only; likewise, the findings of the evaluation will be used for research purposes only and may be published in academic publications. Your privacy will be protected by not printing any names, positions, or institutions in any such publication. The data will be stored in a password-protected computer and locked file cabinet at Unisa for a period of five years, after which it will be incinerated.

Please tick the checkbox to voluntarily provide consent to participate in the study.

I accept □

SECTION C: Instructions

All questions marked with an asterisk (*) need to be answered. The information requested in Section D is for verification purposes only and responses will only be identified through a pseudo name/number, with no reference to any individual whatsoever.

Section E consists of the checklist items that system designers need to address. There are 12 usable security principles specifically tailored to online banking service. Each principle has a varying number of checklist items, ranging from five to nine, that help in understanding and applying the principle during the design of the user interface. We request your input in rating the importance of each of the checklist items to determine the usefulness of the principle as a whole. Each checklist item is rated based on a scale with the following four options: very important, important, moderately important, and not important. Evaluators are requested to provide additional information that they think might improve the framework at both a checklist and a principle level.

SECTION D: Biographical information

Please note that the information requested here is for verification purposes only; your responses will only be identified through a pseudo name/number, with no reference to your name whatsoever.

Full name				
Gender	Male		Female	
Age				
Qualification				
Occupation				
Job title				
Job specialisation				
Years in position				
IT/IS security experience				
Usability/UX experience				
Usable security experience				
Other experience (please specify)				

SECTION E: Checklist items

Your assessment is based on the importance of the 12 principles and their respective checklist items in addressing security and usability aspects of system development. Additional comments are welcome at both a checklist item and a principle level.

Please indicate your choice by selecting one of the provided options as follows: 1 = Not important, 2 = Moderately important, 3 = Important, and 4 = Very important.

1	**Visibility: the system should visibly keep users informed about their security status**
	Checklist items
1.1	Does the system show the user the progress status during a visible delay in response time?
1.2	Does the system visibly show the current selection/data input field?
1.3	Does the system clearly highlight the problem field with regard to error messages?
1.4	Is there some form of feedback for every security-related action?
1.5	Does the system visibly show the location of security-related options?
1.6	Is help information for assisting the user visible and easily accessible?
	Additional comments (optional)
2	**Learnability: the system should ensure that security actions are easy to learn and remember**
	Checklist items
2.1	Does the system provide easy-to-learn training material?
2.2	Is there a quick-start guide to assist the user?
2.3	Are security and non-security operations easy to learn and use?
2.4	Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?
2.5	Does the system present security and non-security information in a standardised format?
2.6	Are security options selected by default?
2.7	Does the user interface make it obvious which security items are currently selected?
2.8	Does the system protect users against making severe errors?
	Additional comments (optional)

3	**Errors: the system should provide users with detailed security error messages that they can understand and act on**
	Checklist items
3.1	Are system error messages grammatically correct and accurate in stating the problem, with enough information for corrective measures/actions?
3.2	Do security-related error messages inform the user of the severity of the error?
3.3	Are menu items arranged logically to prevent users from making serious errors?
3.4	Does the system warn users if they are about to make a potentially serious error?
3.5	Does the system allow users to recover from errors quickly and easily?
3.6	Do the error messages of the system not interfere with the users' work, whenever possible?
3.7	Does the system clearly ask for users' confirmation of serious and possibly irrevocable actions?
	Additional comments (optional)
4	**Availability: system services must be available all the time, with minimum down time, and have minimum interruptions**
	Checklist items
4.1	Is the system always available, with minimum and non-interruptive down time?
4.2	Does the system make sure that all system functionalities are available at all times?
4.3	Is scheduled down time communicated in advance and scheduled during off-peak times?
4.4	Does the system limit the frequency of changes to the user interface?
4.5	Do updates to the system user interface not result in users having to learn the system all over again?
	Additional comments (optional)
5	**Satisfaction: the system should ensure that users have a good experience when using the system and its security features**
	Checklist items
5.1	Is the actual process of using the system fun and enjoyable?
5.2	Are the most frequently used function keys in the most accessible positions?

5.3	Do security-related prompts imply that the user is in control?
5.4	Is each individual security setting a member of a family of security options?
5.5	Do the security mechanisms of the system provide a sense of protection to the user?
5.6	Has colour been used specifically to draw attention, communicate organisation, indicate status changes, and establish relationships for security- and non-security-related actions?
5.7	Can users personalise their own system, session, file, and screen defaults, such as the landing page?
5.8	Does the system fulfil its claimed capabilities?
5.9	Does the system complete unambiguous partial input on a data entry field?
	Additional comments (optional)
6	**Revocability: the system should allow users to revoke any of their security actions**
	Checklist items
6.1	Do security options in menus make it obvious whether deselection is possible?
6.2	Can users easily reverse their security and non-security actions?
6.3	When prompts imply a necessary security action, are the words in the message consistent with that action?
6.4	Has the system been designed so that keys with similar names do not perform opposite (and potentially dangerous) security actions?
6.5	Can users cancel operations in progress?
6.6	Are there ‘undo’ and ‘redo’ functions at the level of a single security action or for a complete group of security actions?
6.7	Does the system provide confirmation for actions that have drastic, possibly destructive consequences?
6.8	Does the system have a clearly marked exit?
	Additional comments (optional)
7	**Expressiveness: the system should guide users on security in a manner that still gives them freedom of expression**
	Checklist items

7.1	Are users initiators of security actions rather than respondents?
7.2	Does the system correctly anticipate, and prompt for, the user's probable next security-related activity?
7.3	By looking, can the user tell the security state of the system and the alternatives for security-related actions, if needed?
7.4	Does the system clearly state its security capabilities?
7.5	Does the system clearly state the users' responsibilities in terms of security actions?
	Additional comments (optional)
8	**User language: the system should use plain language that users can understand with regard to security**
	Checklist items
8.1	Does the system allow the user to choose a preferred language?
8.2	Are security actions and objects named consistently across all prompts in the design?
8.3	Is security information accurate, complete, and understandable?
8.4	Are security questions stated in clear and simple language, where used?
8.5	If language selection is possible, is the translation accurate, without errors?
	Additional comments (optional)
9	**User suitability: the system should provide options for users with diverse levels of skill and experience in security**
	Checklist items
9.1	Is security information accurate, complete, and understandable to all types of system users (experienced and novice)?
9.2	Can users define and group their own synonyms for commands for easier access?
9.3	Can users navigate forwards and backwards within operations?
9.4	Does the system avoid the use of security and privacy jargon?
9.5	If the system supports both novice and expert users, are multiple levels of error message detail available?
	Additional comments (optional)

10	**Help and documentation: the system should make security help apparent and easy to find for users**
	Checklist items
10.1	Is the help function visible, for example, a key labelled HELP or a special menu?
10.2	Is it easy to access, and return from, the help function, allowing users to resume their work from where they left off after accessing help?
10.3	Does the help function cover security- and non-security-related information?
10.4	Does the system provide an up-to-date security centre, with security training and awareness information?
10.5	Does the system provide a 24-hour help desk for critical security incidents?
10.6	Does the system provide complete and accurate help and a FAQs section?
10.7	Is the help and FAQs material searchable and grouped in logical categories?
10.8	Does the system provide detailed training and education material on how to complete basic tasks?
10.9	Does the system provide a search function for locating system functions?
	Additional comments (optional)
11	**Security: the system should provide trusted communication channels between the user and the data servers**
	Checklist items
11.1	Do critical transactions require out-of-band authentication such as an OTP/SMS?
11.2	Does the system initiate a session lock after a period of inactivity or on user request?
11.3	Does the system employ encryption techniques to prevent unauthorised disclosure of, and access to, information in storage and transmission?
11.4	Does the system enforce a limit on consecutive invalid access attempts by a user during a period of time?
11.5	Does the system implement an appropriate time-out logoff period?
11.6	Does the system encrypt passwords in storage and in transmission?
11.7	Does the system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.?

11.8	Are system password requirements complex enough to avoid simple password-cracking attacks?
	Additional comments (optional)
12	**Privacy: the system should protect user information against unauthorised access by third parties**
	Checklist items
12.1	Does the system ask for consent before collecting personal information?
12.2	Are the statements asking for user consent written in clear and simple language that the user understands?
12.3	Does the system clearly state what personal information is collected and for what purposes it will be used?
12.4	Does the system require users to confirm statements indicating that they understand the conditions of access?
12.5	Does the system ask for permission before distributing personal information to third parties?
12.6	Do the personal information collection and storage mechanisms comply with the data protection regulations of the country?
12.7	Can protected or confidential areas be accessed with certain passwords?
	Additional comments (optional)

Thank you very much for your participation

Thank you once again for your participation and please feel free to contact me or the study promoters with any questions on the contact details below:

Mr M Mujinga, School of Computing, College of Science, Engineering, and Technology, Unisa, mujinm@unisa.ac.za

Prof. MM Eloff, Institute for Corporate Citizenship, College of Economic and Management Sciences, School of Computing, Unisa (promoter)

Prof. JH Kroeze, School of Computing, College of Science, Engineering, and Technology, Unisa (co-promoter)

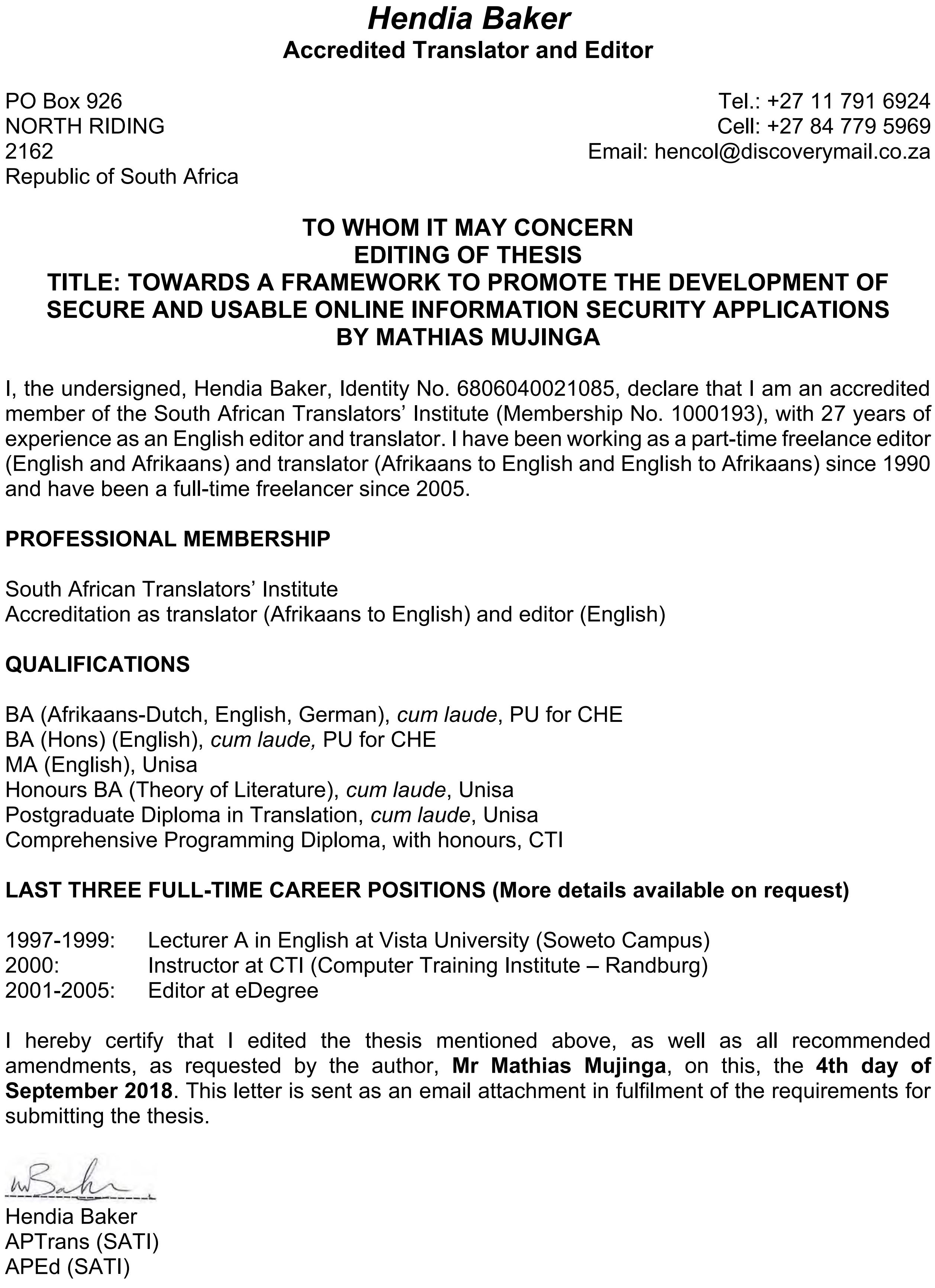
Appendix M: Framework evaluation results sample

Please tick the checkbox	2. Gender:	3. Age:	4. Highest educational qualification	5. Occupation:	6. Job title:	7. Job specialisation:	8. Years in position:
I accept	Female	51 years or older	Postgraduate degree	Lecturer	Lecturer	Information System	11 years
I accept	Male	41-50 years	Postgraduate degree	Lecturer	Lecturer	teaching, research and community engagement	15
I accept	Male	31-40 years	Postgraduate degree	Tester	Test Analyst	Software Testing	2
I accept	Male	31-40 years	Postgraduate degree	Information Technology	Computer Technician	Desktop Support	8
I accept	Female	31-40 years	Post-matric certificate or Diploma	Information Security Architect in financial industry	Lead Information Security Architect	Design information security roadmap and strategy	10
I accept	Male	31-40 years	Postgraduate degree	Head IT: Quality Assurance	Head of Quality Assurance	Software Quality Assurance	5 and six months
I accept	Male	31-40 years	Postgraduate degree	Academia	Lecturer	Information security	10
9. IT/IS security experience:	10. Usability/UX experience:	11. Usable security experience:	12. Other experience (please specify):	1.1 Does the system show the user the progress status during a visible delay in response time?	1.2 Does the system visibly show the current selection/data input field?	1.3 Does the system clearly highlight the problem field with regard to error messages?	1.4 Is there some form of feedback for every security-related action?
Intermediate	Expert	Intermediate	UI (User Interface experience) the design of the interaction points between user and system	4	3	3	3
Intermediate	Expert	Intermediate		4	4	4	4
Beginner	Beginner	Beginner		2	2	3	3

Intermediate	Intermediate	Intermediate	Networking	4	4	3	4
Expert	Expert	Expert	Systems integration and application development and design	2	3	1	2
Expert	Expert	Expert	Business Management	3	3	4	3
Expert	Expert	Expert	none	4	4	3	4
1.5 Does the system visibly show the location of security-related options?	1.6 Is help information for assisting the user visible and easily accessible?	Additional comments (optional)	2.1 Does the system provide easy-to-learn training material?	2.2 Is there a quick-start guide to assist the user?	2.3 Are security and non-security operations easy to learn and use?	2.4 Have security items been grouped into logical zones, and have headings been used to distinguish between the zones?	2.5 Does the system present security and non-security information in a standardised format?
4	4		4	4	3	3	3
4	4		4	4	4	4	4
3	3		3	3	2	3	2
3	4		4	3	4	4	4
4	4	Giving end user precise feedback of security errors that occurred exposes the system to potential threats. As a bank we never specify which authentication credential was incorrect for example, we just reply that username password did not match, telling the user that only the password was wrong,	3	3	3	1	3

		makes the system easier to exploit for brute-force attack vectors.					
4	3	System has to be user friendly and direct users as to where to correct populated details	3	3	3	4	3
4	3		2	1	4	4	4
2.6 Are security options selected by default?	2.7 Does the user interface make it obvious which security items are currently selected?	2.8 Does the system protect users against making severe errors?	Additional comments (optional)	3.1 Are system error messages grammatically correct and accurate in stating the problem, with enough information for corrective measures/actions?	3.2 Do security-related error messages inform the user of the severity of the error?	3.3 Are menu items arranged logically to prevent users from making serious errors?	3.4 Does the system warn users if they are about to make a potentially serious error?
3	3	3	The learnability principle is very important especially to the older generation.	3	3	3	3
2	3	4		4	4	3	3
3	2	3		3	4	3	3
4	3	4		4	3	3	4
2	3	4		2	2	3	2
3	4	4		4	4	4	4
4	4	4		3	4	4	4

Appendix N: Certificate of language editing



Hendia Baker

Accredited Translator and Editor

PO Box 926
NORTH RIDING
2162
Republic of South Africa

Tel.: +27 11 791 6924
Cell: +27 84 779 5969
Email: hencol@discoverymail.co.za

TO WHOM IT MAY CONCERN
EDITING OF THESIS
TITLE: TOWARDS A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS
BY MATHIAS MUJINGA

I, the undersigned, Hendia Baker, Identity No. 6806040021085, declare that I am an accredited member of the South African Translators' Institute (Membership No. 1000193), with 27 years of experience as an English editor and translator. I have been working as a part-time freelance editor (English and Afrikaans) and translator (Afrikaans to English and English to Afrikaans) since 1990 and have been a full-time freelancer since 2005.

PROFESSIONAL MEMBERSHIP

South African Translators' Institute
Accreditation as translator (Afrikaans to English) and editor (English)

QUALIFICATIONS

BA (Afrikaans-Dutch, English, German), *cum laude*, PU for CHE
BA (Hons) (English), *cum laude,* PU for CHE
MA (English), Unisa
Honours BA (Theory of Literature), *cum laude*, Unisa
Postgraduate Diploma in Translation, *cum laude*, Unisa
Comprehensive Programming Diploma, with honours, CTI

LAST THREE FULL-TIME CAREER POSITIONS (More details available on request)

1997-1999:	Lecturer A in English at Vista University (Soweto Campus)
2000:	Instructor at CTI (Computer Training Institute – Randburg)
2001-2005:	Editor at eDegree

I hereby certify that I edited the thesis mentioned above, as well as all recommended amendments, as requested by the author, **Mr Mathias Mujinga**, on this, the **4th day of September 2018**. This letter is sent as an email attachment in fulfilment of the requirements for submitting the thesis.

Hendia Baker
APTrans (SATI)
APEd (SATI)

Appendix O: Certificate of statistical analysis

31 AUGUST 2017

RE: STATISTICAL ANALYSIS OF THE QUANTITATIVE DATA ANALYSIS

To Whom It May Concern

This letter serves to inform and confirm that I, Edzai Kademeteme was involved in empirical research statistical analysis of the doctoral dissertation by Mathias Mujinga titled: 'TOWARDS A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS'. I can verify and vouch for the accuracy of the quantitative statistical techniques used in this research.

If there is any information that you might require from me please do not hesitate to contact me on details below.

Yours truly,

Edzai Kademeteme
MTech (Business Information Systems)
eamkademeteme@gmail.com
+27 73 959 7973

Appendix P: Certificate of transcription

Certificate of Transcriptions

Peter T. Mekgwe
Unit 22 Protea Glen Complex
Kina Street
Weltevreden Park
1739

21 August 2017

This is to certify that I Peter T. Mekgwe I am an experienced and accredited member of the South African Translator's Institute for the last 18 years (Registration No. 1000281).

I have to the best of my ability provided a true and accurate transcription of the source audio files for Mathias Mujinga's interview data for the thesis titled: 'TOWARDS A FRAMEWORK TO PROMOTE THE DEVELOPMENT OF SECURE AND USABLE ONLINE INFORMATION SECURITY APPLICATIONS' during the course of the year 2016.

Signed: ____________ PETER MEKGWE

AUGUST 2017

Tel: (011) 782 5474 | Mobile: 072 519 0506
brainstorming@vodamail.co.za | petertmekgwe@gmail.com