A Framework to Evaluate User Experience of End user Application Security Features

By

Fungai Bhunu Shava

2016

A Framework to Evaluate User Experience of End user Application Security Features

By

Fungai Bhunu Shava

Thesis

Submitted in fulfilment of the requirements for the degree

Philosophiae Doctor

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

at the

Nelson Mandela Metropolitan University

April 2016

Promoter: Professor Darelle van Greunen

DEPARTMENT OF ACADEMIC ADMINISTRATION
EXAMINATION SECTION
SUMMERSTRAND NORTH CAMPUS
PO Box 77000
Nelson Mandela Metropolitan University
Port Elizabeth
6013

Enquiries: Postgraduate Examination Officer

Nelson Mandela Metropolitan University
for tomorrow

DECLARATION BY CANDIDATE

NAME: **Fungai Bhunu Shava**

QUALIFICATION: **DOCTOR PHILOSOPHIAE: INFORMATION TECHNOLOGY**

TITLE OF PROJECT: **A Framework to Evaluate User Experience of End user Application Security Features.**

DECLARATION

In accordance with Rule G 4.6.3, I, Fungai Bhunu Shava with student number 212386336, hereby declare that the above stated thesis for the degree Philosophiae Doctor: Information Technology is my own work and that it has not previously been submitted for assessment to another University or for any other qualification.

Signature:  Date: 30 December 2015

ACKNOWLEDGEMENTS

I thank Almighty God, my strength, my guide and my source of wisdom, health, anointment and guidance. When I was weary you energised me, when I was confused you directed me.

I am grateful for the support and mentorship received during my journey from the following:

Prof. Darelle van Greunen, my supervisor, promotor, mentor, leader and friend: You, like a fisherman, sought me in the big ocean, and made it your business to see my dream come true. You did not concern yourself with my academic growth only, but also with my welfare. You saved my health through a conversation which was not between student and supervisor but between friends; you provided guidance in all spheres in my life. You led me through the journey of discovering my true passion, which otherwise I would have never been able to realise: HCI, in particular UX. You were and are an inspiration for me to live a selfless life through acts of service to those within my sphere of influence.

Participants: I thank you all for the priceless gift of time that you committed to make this journey a success. Without you, this research would have been impossible.

Expert reviewers: Your expertise and time is highly valued as it helped me to unveil issues that need to be addressed to make user experiences secure and enjoyable.

Friends: Without your support, encouragement and critique, this journey would have been a nightmare. Thank for being there for me when I needed you the most.

My family: Special thanks to all my family for their support throughout the journey. Patridge, my husband, I thank you for your patience, confidence in me, support and love that helped me to trudge through the rocky days. Marlven, Ralph and Clive, my lovely sons, I thank you for understanding and giving me the space to do my studies. Above all: thank you for the entertainment, trust and the questions that kept me going. To my siblings, Elphas and Sandra, and to mum; thank you for the support and prayers. Anold and Faith, my daughter and sister; your availability to listen, to read, to stand in the gap when the boys needed attention, is valued. God bless you. Patrick, Sara and Edmund: thank you for the encouragement. And to the rest of my family, I cannot mention you all by name, but I value your contributions to the success of this journey.

Polytechnic of Namibia (now the Namibia University of Science and Technology): Thank you for supporting and understanding the need for personal development in me as an employee. Colleagues, your support and encouragement throughout the journey are valued, thank you.

NMMU: Thank you for believing in me and according me the opportunity to study in your prestigious institution. A special thank you goes to the administrative staff, especially International Relations, for your support and responsiveness**.** Last but not least, a special thank you goes to Ms Leornard, the School of IT staff and students for your support and mentorship. It is the likes of you who make the journey possible though the direction arrows you post at every turn on the way!

Peer review of academic publications

Two publications were made at two conferences, namely Information Security South Africa (ISSA2013) and International Development Informatics Association Conference (IDIA2014) and they are presented in Appendix C. The ISSA2013 paper communicated the identified factors that affect user experience of interacting with end user program security features, while the IDIA2014 paper proposed user awareness metrics for establishing baseline organisational security posture in the case site studied. The findings of the two academic papers are among the components of the theoretical framework and the developed EUPSFUX evaluation framework.

Double-blind peer reviewed papers in conference proceedings:

2013

Bhunu Shava, F. and van Greunen, D. *Factors affecting user experience with security features: A case study of an academic institution in Namibia,* IEEE, ISBN 978-1-4799-0808-0/13. Presented at ISSA 2013 (International Information Security South Africa Conference)

2014

Bhunu Shava, F. and van Greunen, D. *Designing user security metrics for a security awareness at Higher and Tertiary institution.* Proceedings of the 8th International Development Informatics Association conference (IDIA 2014). Port Elizabeth. ISBN: 978-0-620-63498-4, 280-296

Chapter in Book

2015

Bhunu Shava, F. and van Greunen, D. Developing User Security Metrics towards Awareness Creation. Chapter 10 in ICTs for Inclusive Communities in Developing Societies. Cambridge Scholarly Publications. Eds Steyn and Van Greunen. ISBN 1-4438-8081-7

ABSTRACT

The use of technology in society moved from satisfying the technical needs of users to giving a lasting user experience while interacting with the technology. The continuous technological advancements have led to a diversity of emerging security concerns. It is necessary to balance security issues with user interaction. As such, designers have adapted to this reality by practising user centred design during product development to cater for the experiential needs of user - product interaction. These User Centred Design best practices and standards ensure that security features are incorporated within End User Programs (EUP). The primary function of EUP is not security, and interaction with security features while performing a program related task does present the end user with an extra burden. Evaluation mechanisms exist to enumerate the performance of the EUP and the user's experience of the product interaction. Security evaluation standards focus on the program code security as well as on security functionalities of programs designed for security. However, little attention has been paid to evaluating user experience of functionalities offered by embedded security features.

A qualitative case study research using problem based and design science research approaches was used to address the lack of criteria to evaluate user experience with embedded security features. User study findings reflect poor user experience with EUP security features, mainly as a result of low awareness of their existence, their location and sometimes even of their importance. From the literature review of the information security and user experience domains and the user study survey findings, four components of the framework were identified, namely: end user characteristics, information security, user experience and end user program security features characteristics.

This thesis focuses on developing a framework that can be used to evaluate the user experience of interacting with end user program security features. The framework was designed following the design science research method and was reviewed by peers and experts for its suitability to address the problem. Subject experts in the fields of information security and human computer interaction were engaged, as the research is multidisciplinary. This thesis contributes to the body of knowledge on information security and on user experience elements of human computer interaction security regarding how to evaluate user experience of embedded InfoSec features. The research adds uniquely to the literature in the area of Human Computer Interaction Security evaluation and measurement in general, and is specific to end user program security features. The proposed metrics for evaluating UX of

interacting with EUP security features were used to propose intervention to influence UX in an academic setup. The framework, besides presenting UX evaluation strategies for EUP security features, also presents a platform for further academic research on human factors of information security. The impact can be evaluated by assessing security behaviour, and successful security breaches, as well as user experience of interaction with end user programs.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION 1

1.1 BACKGROUND 1

1.1.1 General usage of ICT in the work place 1

1.1.2 Impact of better technology access and Internet Connectivity 2

1.1.3 Overview of end user programs typically used in the work place 2

1.1.4 User experience 2

1.1.5 End user program security 5

1.1.6 Usable security 6

1.2 PROBLEM DESCRIPTION 6

1.2.1 Overview 7

1.2.2 Motivation 8

1.3 PROBLEM STATEMENT 8

1.4 RESEARCH OBJECTIVES AND QUESTIONS 9

1.5 SCOPE AND DELINEATION OF RESEARCH 10

1.6 RESEARCH METHODOLOGY 10

1.7 ETHICAL CLEARANCE 12

1.8 RESEARCH SIGNIFICANCE AND CONTRIBUTION 12

1.9 CHAPTER OUTLINE 12

CHAPTER 2: RESEARCH METHODOLOGY 14

2.1 INTRODUCTION 14

2.2 RESEARCH PARADIGMS AND THE PHILOSOPHICAL ASSUMPTIONS 14

2.2.1 Research Paradigm and Philosophical Assumptions Applicable to this Study 16

2.3 RESEARCH STRATEGIES 16

2.4 DESIGN SCIENCE RESEARCH STRATEGY OVERVIEW 17

2.4.1 Design Science Research Products 18

2.4.2 Design Science Research Cognitive Reasoning Processes 19

2.4.3 Design Science Research Methodologies 19
2.4.4 Design Science Research Process models 21
2.4.5 A Three Cycle View of Design Science Research 23
2.4.6 Artefacts Evaluation in Design Science Research 23
2.4.7 Quality of the framework 26
2.4.8 Design Science Research Strategy Application to this Thesis 29
2.4.9 Cycles of the Design Science Research Process 35
2.4.10 Research Cycles to develop the framework 36
2.5 DATA COLLECTION METHODS 37
2.5.1 Case studies 38
2.5.2 Data Analysis 41
2.6 ETHICAL CONSIDERATIONS 43
2.6.1 Ethical consent 43
2.6.2 Anonymity and confidentiality 43
2.7 SUMMARY 43
CHAPTER 3: HUMAN COMPUTER INTERACTION - USER EXPERIENCE 44
3.1 INTRODUCTION 44
3.2 HUMAN COMPUTER INTERACTION 45
3.3 INTERACTION 47
3.3.1 Interaction Design 47
3.3.2 User-Centred Design/Human Centred Design 48
3.3.3 Human computer interaction security (HCISec) 50
3.4 USABILITY 51
3.4.1 Security Usability guidelines: 53
3.4.2 Usable security 55
3.5 USER EXPERIENCE 65
3.5.1 UX models and frameworks 68

3.5.2 UX Design 69
3.5.3 UX Evaluation 69
3.6 UX CRITERIA FOR EUP SECURITY FEATURES (EUPSF) 71
3.7 SUMMARY 73
CHAPTER 4: INFORMATION SECURITY FEATURES 74
4.1 INTRODUCTION 74
4.2 INFORMATION SECURITY 75
4.3 END USER PROGRAM SECURITY FEATURES 77
4.4 PROGRAM SECURITY CHARACTERISTICS 78
4.5 END USER SECURITY 79
4.6 ORGANISATIONAL SECURITY CULTURE 80
4.7 END USER BEHAVIOUR TOWARDS SECURITY 83
4.8 SECURITY PRODUCT EVALUATION METHODS AND CRITERIA 84
4.8.1 Security usage 85
4.8.2 Security metrics 86
4.9 SUMMARY 89
CHAPTER 5: DATA COLLECTION AND FINDINGS 91
5.1 INTRODUCTION 91
5.2 DATA COLLECTION PLANNING 92
5.2.1 Overview of the case study 92
5.2.2 Sampling 92
5.3 DESIGNING THE DATA COLLECTION 93
5.3.1 Research instruments used 93
5.3.2 Designing of the instruments 93
5.4 PREPARATION FOR THE DATA COLLECTION 95
5.4.1 Permission to carry out research 95
5.4.2 Pilot studies: Data collection method 1: semi-structured interviews 95

5.4.3 Data collection method 2: Policy document reviews 95
5.4.4 Survey validation 96
5.4.5 Data collection method 3: Survey pre-test 98
5.5 DATA COLLECTION 98
5.5.1 Data collection plan 98
5.5.2 Data collected 98
5.5.3 Summary of findings 112
5.5.4 Security awareness approach 114
5.6 CASE STUDY VALIDATION 119
5.7 SUMMARY 120
CHAPTER 6: FRAMEWORK DESIGN 122
6.1 INTRODUCTION 122
6.2 FRAMEWORKS 123
6.2.1 Types of frameworks and definitions 124
6.2.2 Types of conceptual frameworks 126
6.2.3 Purpose of conceptual frameworks 127
6.2.4 Presentation of conceptual frameworks 127
6.2.5 Limitations of conceptual frameworks 128
6.2.6 Conclusion 128
6.3 EUPSFUX METHODOLOGICAL DESIGN PROCESS 128
6.3.1 Phase 1- Identify problem and motivate 129
6.3.2 Phase 2 - Define objectives of a solution 131
6.3.3 Phase 3 - Design and development 133
6.3.4 Phase 4 - Demonstration 150
6.3.5 Phase 5- Framework evaluation 154
6.3.6 Phase 6- Communication 155
6.4 SUMMARY 156

CHAPTER 7: FRAMEWORK FINALISATION 158
7.1 INTRODUCTION 158
7.2 EUPSFUX FRAMEWORK EVALUATION 158
7.2.1 Evaluation tools 159
7.2.2 Quality of the EUPSFUX framework 159
7.2.3 Reliability/Dependability 161
7.2.4 Relevance 161
7.2.5 Theoretical validation 161
7.2.6 Heuristic evaluations 161
7.2.7 Expert review: Tentative framework evaluation 186
7.3 REFINED EUPSFUX FRAMEWORK 187
7.4 FRAMEWORK LIMITATIONS 190
7.5 SUMMARY 190
CHAPTER 8: OVERALL RESEARCH CONCLUSION 191
8.1 INTRODUCTION 191
8.2 RESEARCH CONTRIBUTIONS 192
8.2.1 Contribution 1: Framework design process 194
8.2.2 Contribution 2: Framework implementation guideline 194
8.2.3 Contribution 3: EUPSFUX framework 194
8.2.4 Contribution 4: Framework evaluation toolset 195
8.2.5 Heuristic evaluation 195
8.2.6 Awareness metrics 196
8.3 REFLECTION 196
8.3.1 Methodological reflection 196
8.3.2 Scientific reflection 197
8.3.3 Substantive reflection 198
8.4 LESSONS LEARNT 198

8.5 RESEARCH LIMITATIONS 199
8.6 FUTURE DIRECTIONS 199
8.7 CONCLUDING REMARKS 200
REFERENCES 203
Appendix A1: Online Survey questionnaire 225
Appendix A2: Permission to conduct study 239
APPENDIX A3: Cover letter 240
Appendix A4: Semi-structured interviews 242
Appendix A5: Survey results summary 243
Appendix A6: Survey Raw Data 244
Appendix B1: Checklist for Adobe Reader 245
Appendix B2: Checklist for MS Word 252
Appendix B3: Cross comparison of Adobe and MS Word 259
Appendix C1: Conference paper 1 263
Appendix C2: Conference paper 2 272
Appendix C3: Book chapter 288
Appendix C4: Editor's Letter 309

List of abbreviations

BMIS	Business Model for Information Security
BYOD	Bring Your Own Device
DSR	Design Science Research
DSRM	Design Science Research Methodology
EU	End User
EUP	End User Program
EUPSF	End User Program Security Features
EUPSFUX	End User Program Security Features User Experience
HE	Heuristic Evaluation
HCI	Human Computer Interaction
HCI-Sec	Human Computer Interaction Security
ICT	Information Communication Technology
ID	Interaction Design
IE	Internet Explorer
IS	Information security
IT	Information Technology
InfoSec	Information Security
MS	Microsoft
PC	Personal Computer

PDF	Portable Document Format
PoN	Polytechnic of Namibia
SF	Security Features
UB	User Behaviour
UCD	User Centred Design
USec	Usable Security
UX	User Experience

List of Figures

Figure 1-1: Components of user experience 4
Figure 1-2: Actual usability and UX model 7
Figure 1-3: Thesis layout 13
Figure 2-1: DSR Methodology adopted from 18
Figure 2-2: DSR Process 22
Figure 2-3: Three cycle view of DSR 23
Figure 2-4: DSRM process for the EUPSFUX framework 30
Figure 2-5: Problem identification 32
Figure 2-6: DSR cycles applied to thesis 36
Figure 2-7: Data collection process 37
Figure 3-1: Disciplines of the HCI field modification of 45
Figure 3-2: UCD activities 49
Figure 3-3: Elements of the model of interaction from the designer and user perspectives 53
Figure 3-4: Security - usability threat model 58
Figure 3-5: Modified usability framework 59
Figure 3-6: UX research progress 65
Figure 3-7: Simplified model of User Experience 67
Figure 3-8: Awareness UX model 68
Figure 3-9: Snapshots during interaction 71
Figure 4-1 Business model for information security (BMIS) 76
Figure 5-1: End user awareness of security threats 104
Figure 5-2: Security training 105
Figure 5-3: Source of help 106
Figure 5-4: Feelings towards acting on security messages 107
Figure 5-5: Email clients 110
Figure 5-6: Theoretical framework 113
Figure 5-7: Where users learn about security policies 117
Figure 5-8: Security awareness roadmap adopted from SANS 118
Figure 6-1: Composition of a framework 125
Figure 6-2: EUPSFUX methodological design process 129
Figure 6-3: Phase 1 of the EUPSFUX methodological process 130
Figure 6-4: Phase 2 of the EUPSFUX methodological approach 132

Figure 6-5: Phase 3 of the EUPSFUX methodological approach....134
Figure 6-6: End user characteristics....136
Figure 6-7: EUPSF relative to InfoSec and EUP....137
Figure 6-8: UX relative to other constructs....138
Figure 6-9: Factors affecting InfoSec....139
Figure 6-10: Construct interrelationships....140
Figure 6-11: User awareness - UX relationship....141
Figure 6-12: EU characteristics and IS....142
Figure 6-13: InfoSec-UX relationship....143
Figure 6-14: All components relatedness....144
Figure 6-15: Conceptual relationship....145
Figure 6-16: Framework evaluation derivation process....146
Figure 6-17: Implementation of the framework....147
Figure 6-18: Tentative framework composition for UX experts....148
Figure 6-19: EUPSFUX framework....149
Figure 6-20: Phase 4 of the EUPSFUX methodological approach....150
Figure 6-21: Phase 5 of the EUPSFUX methodological approach....154
Figure 6-22: Evaluation process....155
Figure 6-23: Phase 6 of the EUPSFUX methodological process....156
Figure 7-1: Refined framework....189

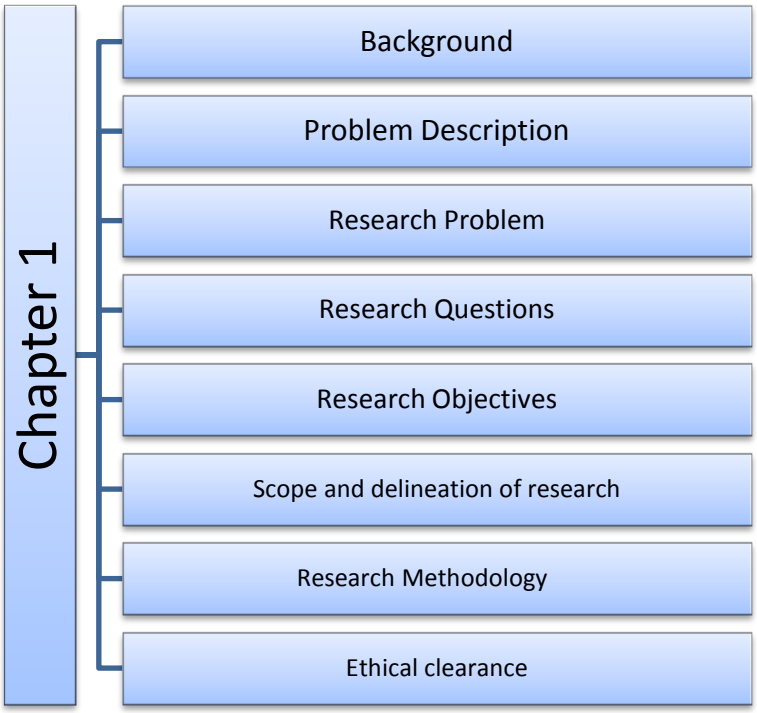
List of Tables

Table 1-1: Research methods used to answer research questions....11
Table 2-1: Research philosophies and associated reasoning....15
Table 2-2: Research Outputs of DSR....19
Table 2-3: Research: DSR guideline....21
Table 2-4: DSR evaluation methods....24
Table 2-5: Selected framework evaluation criteria per domain....25
Table 2-6: Framework development process....31
Table 2-7: Research objective and corresponding questions....33
Table 3-1: Typical usability inquiry methods....61
Table 3-2: Standardised questionnaires....62
Table 3-3: Typical usability inspection methods....63
Table 3-4: Proposed criteria....72
Table 4-1: InfoSec behaviour modes....83
Table 4-2: Design principles....86
Table 4-3: Top down approach....88
Table 4-4: Bottom up approach....88
Table 5-1: Participants' representation by gender....99
Table 5-2: Respondents' affiliation....99
Table 5-3: Participants' employment period in the case site....100
Table 5-4: Summary of survey findings....101
Table 5-5: UX with security threats....105
Table 5-6: Frequency of using security technology....108
Table 5-7: Program usage....108
Table 5-8: Uses of the computer....109
Table 5-9: Feelings about notifications and alerts handling....111
Table 5-10: Bottom-up approach employed for analysis of results....115
Table 5-11: Knowledge of policies....116
Table 5-12: Calculated risk rating for security policy awareness....117
Table 5-13 Security awareness metrics....119
Table 5-14: Case study validity....120
Table 6-1: Summary of framework types....124
Table 6-2: Component descriptions....126

Table 6-3: Constructs and components 135
Table 6-4: Framework implementation demonstration 152
Table 7-1: EUPSFUX framework evaluation tools 159
Table 7-2: EUP compliance to selection criteria 164
Table 7-3: Security features in Adobe and MS Office 165
Table 7-4: Improvements on the HE 167
Table 7-5: Expert and peer reviewer profiles 170
Table 7-6: Adobe heuristic evaluation 171
Table 7-7: Summary of extents of usability per item 177
Table 7-8: Word heuristic evaluation 179
Table 7-9: Expert demographics 187
Table 7-10: Framework development process evaluation 188
Table 8-1: Research question, answers and evidence 200

CHAPTER 1: INTRODUCTION

The first chapter will introduce the thesis following the outline as indicated below.



1.1 BACKGROUND

1.1.1 General usage of ICT in the work place

Information Communication Technology (ICT) has become an integral component of all business sectors and homes. It is providing a platform for education, marketing, innovation and networking. Workplaces are driven by modern ICT devices and products as they have become readily available to most people and businesses. Devices include Tablet PCs, iPods, iPhones, PDA, PCs, etc. There have been tremendous technological advancements globally; however, this thesis focuses on Namibia. The Namibian industry is driven by ICT and the national agenda for vision 2030 and national development plan 4 (NDP4) focus on integrating ICTs in all schools. In order to realise this dream more devices are being deployed to schools (Isaacs, 2007). Most jobs and communication now depend on information technology and are carried out with the aid of some end user application program.

1.1.2 Impact of better technology access and Internet Connectivity

Advancements in both system design and communication technologies have presented an opportunity for all to be interconnected. Interconnection provides educational, social and economic benefits to individuals, organisations and communities. Among the benefits are collaboration, resource sharing, convenience, high productivity, efficiency, availability, interaction, cost management and optimisation (Milligan, 2006). Employees are no longer office bound as they can access their workplace resources from home and deliver their work within stipulated times. This is enabled by the use of a variety of devices, some of which are mobile devices. With the launching of the West Africa Cable System (WACS), it is anticipated that Internet connection rates will drop allowing more Namibians to connect to the Internet (Statistics, Internet World, 2011). According to Telecom Namibia, since 2012 they have been doubling the bandwidth at the same rate, this has resulted in a 75% drop in the rates per bandwidth package (Laban, 2016). More information will be shared across the nation and globally. However, the same means of connecting to the Internet are also available to cybercriminals as they are to security novices and experts alike. This poses a security concern as cyber criminals are also going to find it easier to connect, and to access the shared information by manipulating easier targets (SANS, 2011).

1.1.3 Overview of end user programs typically used in the work place

End user applications are the programs that end users employ to perform daily tasks on their computers. The most popular end user programs, documented by Furnell, Jusoh, and Katsabas (2005) are web browsers (Internet Explorer), email client (Outlook Express) and word processors (Microsoft Word). In another study, Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office were also identified as popular application programs (SANS, 2011; SANS, 2011). Most of these popular applications have been identified as easy targets for cyber-attacks. This is achieved by means of influencing human behaviour through the application security.

1.1.4 User experience

User Experience (UX) is the field of Human Computer Interaction (HCI) that focuses on “a person's perceptions and responses that result from the use or anticipated use of a product, system or service” (ISO 9241-210, 2010). Human-Computer Interaction (HCI) is concerned with the design, evaluation and implementation of interactive computing systems for human

use (Hewett, et al., 1992). UX is the intersection of HCI, USec and user behaviour. There are three main UX approaches, as identified by Hassenzahl and Tractinsky (2006) namely:

1. Beyond the instrumental: evaluates interaction /usability aspects focusing on behaviour and establishes link with non-instrumental needs.
2. Emotion and affect: emotions as a consequence of interaction.
3. The experiential: holistic view of UX in a temporal situational context.

Each one is adapted to suit the given scenario. This study focuses on the perceptions and responses of users resulting from their interaction with end user application program security features. The third approach appeals more in this context as it takes cognisance of the context of the UX. To have a holistic view of UX, it is important to consider yet another definition: "a result of user's and product's characteristics when they interact under particular circumstances" (Hassenzahl & Tractinsky, 2006).

The question is: what characteristics does a product have and how do they affect the user? What characteristics does a user have that influence the experience with the features? Focus can be on how the environment, security culture and duties of users shape their emotions when confronted with a dialogue that requires them to act in a secure manner. In their design of usable security, are the designers considering these factors? Hassenzahl (2004) developed a model of UX that describes both the designer's and the user's perspectives of product features discussed in Chapter 3 (Figure 3-3). A designer has an intended product character during development and makes use of guidelines for the user to follow in order to get the desired experience (Hassenzahl, 2004). However, the user has characteristics that shape how the end user perceives the product. Hence, the actual product character they encounter is different from that intended. In turn, this evokes different consequences. Frameworks of UX, including influencing factors, were developed and are defined in terms of the level of negative or positive emotions experienced in a specific context while or after using a product (Schulze & Krömker, 2010; Mathiasen & Bodker, 2008). The framework recognises the role played by human needs in an interaction. This can be used to evaluate the positive or negative emotions resulting from using a security feature and how it motivates future use. The evaluation helps us to determine how the interaction with security features can be guided to ensure a "*degree to which specified users can achieve actual usability, safety, and satisfaction in use in a specified context of use*" (Lew, Olsina, & Zhang, 2010).

This research considers UX with security features, as well as human behaviour towards security, in order to address security problems associated with end user program security features. User behaviour is influenced by many factors such as a lack of knowledge, prioritizing their work targets and misconceptions regarding security threats, among others (Herzog & Shahmehri, 2007). To understand user behaviour, it is important to consider theories of human behaviour such as the theory of reasoned action that considers attitudes towards the action and subjective norms regarding the action (Ajzen & Fishbein, 1980). Attitudes and norms are affected by external factors like personality and demographic traits. Behaviour intention or motivation is a product of attitudes (positive or negative emotions about an act or behaviour) and subjective norms (individual perceptions) (Fishbein & Ajzen, 1980). In 1991, Ajzen added self-efficacy as a third input to behaviour intention and came up with the theory of planned behaviour. Figure 1-1 depicts a framework developed by Minge (2008) showing the diverse components of UX and how they influence the appraisal of the product and subsequent usage behaviour. It summarises most of the aspects of UX discussed this far.

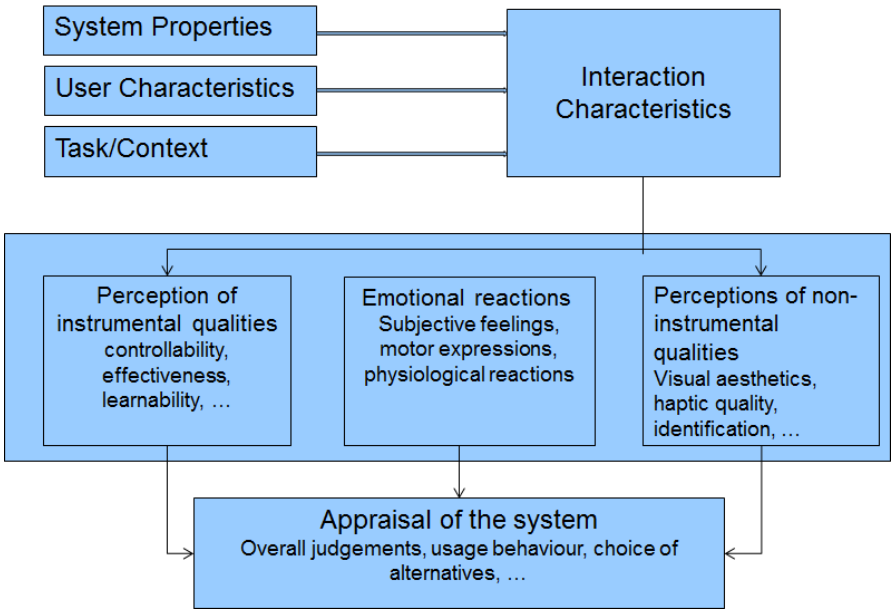


Figure 1-1: Components of user experience (Minge, 2008)

How then can UX of an interaction with application security features in any environment be measured in order to understand the determinant of behaviour intentions?

In order to evaluate the effect of a program's security feature on UX, various criteria that influence the overall UX can be used. Some important aspects are security policies, usability

(convenience, efficiency, understandability, visibility) (Furnell et al., 2005), user knowledge of security threats and solutions and/or mitigation strategies related to their application programs. UX metrics include being enjoyable, fun, helpful, entertaining, satisfying, rewarding, motivating, and pleasing (Hassenzahl, 2004; Schulze & Krömker, 2010).

The end user is the key to information security; hence, it is critical to address their experiences (UX) with security feature interaction in order to address organisational security problems.

1.1.5 End user program security

Information Security is concerned with procedures, people, devices and the communication of information in an integral and confidential way (Whitman & Mattord, 2011). To protect the end user's information, developers of end user programs have embedded security features in the applications. Some of these features interact with users to protect their information while others run in the background (Furnell et al., 2005). The security features are designed to protect individual and organisation security from cyber criminals. However, users fail to use them in the intended manner and present themselves as easy targets for cyber-attacks (Whitman & Mattord, 2011; SANS, 2011). Users cancel updates or disable alerts hence they remain with outdated and unpatched programs.

Program end users regard security as an administrative function that must be handled by Information Technology (IT) technicians. Security related responsibilities are usually ignored owing to the complex nature of security and to the fact that it is not the duty of the users (Herzog & Shahmehri, 2007; Furnell, 2004, Furnell et al., 2005). However, users and technicians have distinct roles to play in securing information. The technicians do all the configurations and the end users act on messages displayed on their screens. There is a need for the end users to understand their responsibility in order to exercise it well, as security is not about administrators alone. In the case of home users it is often necessary for them to configure some of the settings, as well as to access rights (privileges) and policies (Furnell, 2007). With the increased use and ownership of mobile devices (Internet of everything), users have multiple devices that they are using to store their information and each of these has its own security challenges. Bring Your Own Device (BYOD) is a trend that has been embraced by many organisations, so if users are not responsible for their own security, who will ensure InfoSec on these devices? Innocent actions performed by end users can result in poor security-related decisions (Pfleeger & Pfleeger, 2007). Consequently, this results in

vulnerable programs and devices which compromise information security at personal and corporate levels, as these are easily manipulated by hackers. The next section will present user behaviour with security.

1.1.6 Usable security

Usable Security (USec) also known as HCI security (HCI-S) is the field that deals with human issues and Information Security (InfoSec), focusing on the design of security that is usable (NRCNA, 2010; Mathiasen & Bodker, 2008). User centred design engineers for InfoSec focus on ensuring the safety of users while doing their work, without being diverted from their core business in using the computer. This approach has taken centre stage in the development of usable program security features to make the interaction secure (Cranor & Garfinkel, 2005).

USec is also defined as "*A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users*" (Herzog & Shahmehri, 2007). Whitten and Tygar (2003) emphasise that security software is usable if end users are fully aware of the security action they need to carry out, can easily find out how to carry it out successfully without making unsafe mistakes and are at ease with the interfaces to keep on using it. The same should apply to security features embedded into the end user programs. A number of factors influence how end users behave. These include the individual as well as technological characteristics and the environment in which they are used (Abbasi, Lew, Rafique, & Li, 2012). Program security features have characteristics that influence the behaviour of users towards the execution or implementation of such features, as presented in Section 4.4 (Hassenzahl, 2004). Usable security ensures that the security characteristics do not influence the user negatively and that the behaviour intention is positive. However, this can only be true if they behave as stipulated by the designer. Metrics to enumerate the usability of security include: visibility, aesthetic minimalist design, learnability and satisfaction (Johnston, Eloff, & Labuschagne, 2003).

In conclusion, there is a need to consider ways in which end users in general can minimise their vulnerability while using end user programs and being connected to the Internet.

1.2 PROBLEM DESCRIPTION

This section presents the research problem addressed by the thesis.

1.2.1 Overview

Literature studies have shown that there is considerable research on evaluating UX usability; however, considerably less on usable security, secure usable software and UX with security. There is limited literature on tools to evaluate user experience associated with usable security and secure user experience. Figure 1-2 is a model composition representing actual usability and actual UX. What is noticeable is the lack of a security element.

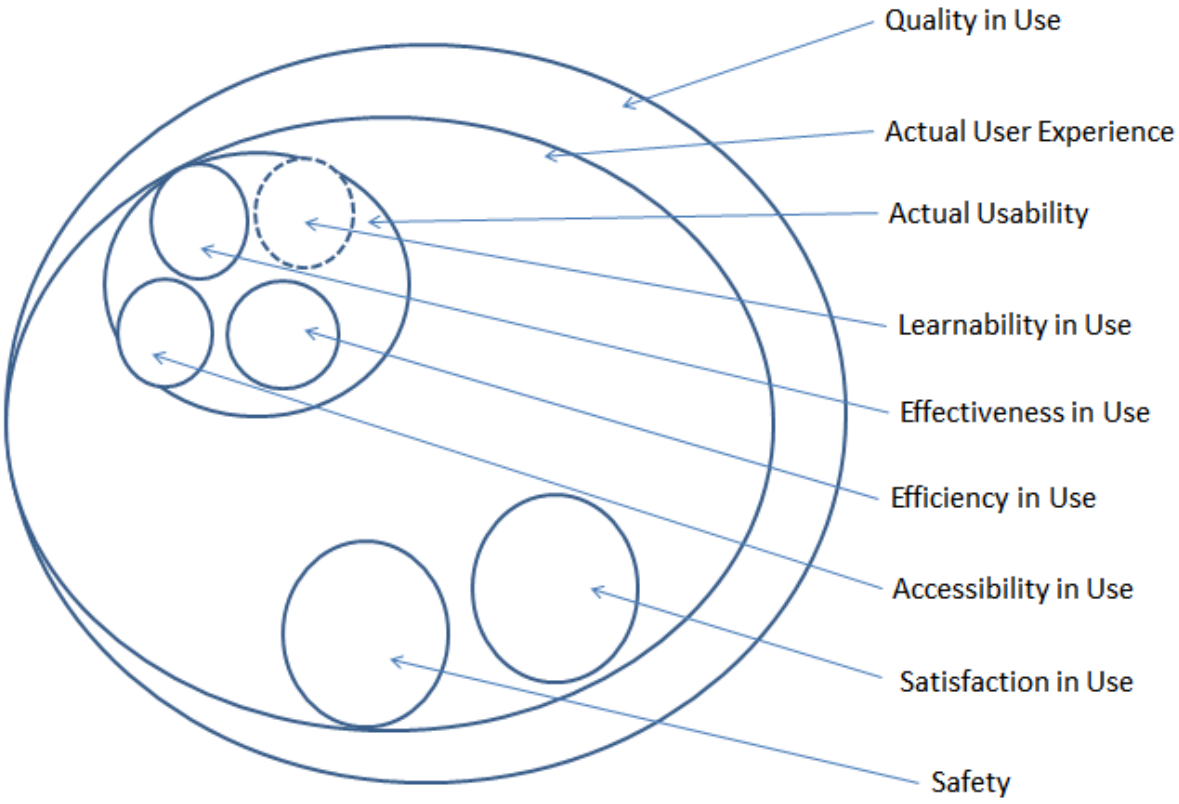


Figure 1-2: Actual usability and UX model (Lew et al., 2010)

To accommodate the missing element, Yeratziotis, Van Greunen, and Pottas (2011) modified Morville's seven facets of UX: useful, usable, desirable, findable, accessible, credible, valuable by including an eighth facet – security. They focused on evaluating usable security in online health systems. Can this modification on UX elements improve end user behaviour with security features? Security interactions do not result in a positive user experience (Furnell, 2010). To establish the scope of the problem, a pilot study was conducted in the case site.

1.2.2 Motivation

A pilot study was conducted at the Polytechnic of Namibia, a tertiary education institution in Windhoek. Semi-structured interviews were used in the pilot study. Semi-structured interviews have major questions which are posed in a similar way to all participants, although the order and level of engagement changed during interaction necessitated by the fact that the researcher already has some idea of the situation and shares a collegial relationship with the interviewees (Crinson & Leontowitsch, 2011).

The semi-structured interviews with five technical staff were conducted to obtain their perception of their users, security status and security awareness level in the population. They reflected that the users are mostly responsible for the problems as a result of poor behaviour and poor adherence to policies. Suggested solutions included centralising the software updates and network access. Active directory and single sign-on were suggested.

In addition to the technical staff, five end users were interviewed to obtain their perspectives on the support they receive from the IT experts supporting them. The results show that they do not enjoy security interaction; they feel that their work is disturbed and that the technicians should perform those functions. However, they do not want the technicians taking time on their computers as this disturbs their work. They seek help from friends and the Internet before calling the helpdesk. They do not really like interacting with security as one option leads to another choice and so on. These findings served as a premise for further studies to be conducted. The pilot study is discussed in more detail in Chapter 5.

1.3 PROBLEM STATEMENT

Based on the findings in literature and the pilot study, the problem statement for this research can be formulated as:

There is a lack of user experience evaluation criteria (metrics) to assess the user experience of end user interaction with embedded security features in end user application programs.

Researchers, such as Furnell et al. (2005), established that negative user experiences with security occur as a result of poor security related decisions and behaviour. The pilot and empirical studies confirmed that there are poor security-related decisions and behaviour with an overall negative experience with Information Security among end users, leaving application programs vulnerable to exploitation by cyber criminals. End user information is

not safe because they do not interact in a secure manner with end user program security features. They remain with negative and insecure emotions/feelings from their interactions; hence, they choose not to interact with the features in future.

Program developers have realised that implementing user centred design approaches in the design of usable security features is not sufficient and have therefore automated many security tasks (Edwards, Poole, & Stoll, 2008). However, it is impossible to by-pass the human element in executing all security tasks; hence, there is always interaction of some sort. Although the features are designed to be usable, end users are still not using them appropriately. Current trends show that application program attacks are still top of the list of security threats with mobile apps leading (SANS, 2011; Lyne, 2014)

1.4 RESEARCH OBJECTIVES AND QUESTIONS

Primary objective:

This research aims to design a framework that can be used to evaluate the user experiences (UX) of interacting with end program security features from a user's perspective.

Specific objectives:

1. To measure the state of UX with end user programs' embedded security features.
2. To determine the suitable security criteria/ methods that can be used to evaluate UX of end user program security features.
3. To determine UX metrics/evaluation criteria can be used to determine the UX of end user program security features.
4. To determine the components and requirements of end user programs' security features' UX and use them to develop the EUPSFUX framework.

Research Questions

The main question to be addressed by this research as the objective is achieved is

How can a framework be designed to evaluate the user experience (UX) of interacting with end user program security features from a user's perspective?

The following four sub-questions support the main research question:

1. What are the factors affecting UX with embedded security features in end user programs?

2. What are the suitable security criteria/ methods that can be used to evaluate UX of end user program security features?
3. Which UX metrics/evaluation criteria can be used to determine the UX of end user program security features?
4. What are the components of a framework to evaluate UX of end user program security features?

1.5 SCOPE AND DELINEATION OF RESEARCH

A case study of the Polytechnic of Namibia was used to design a framework for user experience with end user security features. This study focused on specific end user application programs in use at the Polytechnic of Namibia, namely MS Word and Adobe Acrobat Reader; however, other programs are in use and were not considered owing to popularity of usage. Other active programs were found to be email clients (Pronto, Thunderbird and Outlook), web browsers (Google Chrome, Mozilla Firefox), MS Excel, MS PowerPoint and ITS. The case site uses ICT for their day-to-day business activities. The diversity of professionals in the case calls for the use of a variety of end user programs in executing duties. Each of the programs used has embedded security features, and most or all use web browsers, email clients, PDF and MS Word. Whether or not users interact with these features to protect their information depends on what they expect and how they feel about the interaction. Previous experiences of similar interactions define feelings and attitudes. It is necessary for end users to have secure and positive experiences in order for them to have positive feelings towards future interactions. To evaluate experiences with end user programs, MS Word and Adobe Acrobat Reader were chosen for their adhering to user centred design principles and having a commitment towards positive user experience. A heuristics evaluation tool was designed to assess the identified features in the case programs. Experts and peers performed security tasks using the features and evaluating their performance against a usability, and security checklist. Findings can inform IT, IS and UX experts on what to change as a way of improving user experience of interaction, but better still, they form the basis for designing the framework as they validate the theoretical framework underpinning the study.

1.6 RESEARCH METHODOLOGY

A qualitative research method following an interpretivist research philosophy using inductive reasoning was used to inform the design of an artefact using a design science research paradigm. The artefact in this case is a framework which is discussed in detail in section 6.2.

The area of focus spans the InfoSec as well as UX, Usability and HCISec (USec) domains of HCI; hence, qualitative tools and procedures could address the multidisciplinary nature of the research. A problem based research cycle was followed in defining the research problem. To gather data, validate the theoretical framework and evaluate the usability, security and user experience of end user security features in MS Word and Adobe Acrobat Reader, a case study strategy was found suitable. The cases were purposefully selected because of their richness. Literature reviews, questionnaire surveys, heuristic evaluations and semi-structured interviews were used. Method triangulation was used to improve the quality of the study. For data analysis qualitative strategies such as text analysis, data reduction, coding and data display were used.

Table 1-1: Research methods used to answer research questions

Research question	**Research objective**	**Method**
1. What are the factors affecting UX with embedded security features in end user programs?	To measure the state of UX with end user programs' embedded security features.	Literature survey, case study, survey
2. What are the suitable security criteria/ methods that can be used to evaluate UX of end user program security features? 3. Which UX metrics/evaluation criteria can be used to determine the UX of end user program security features? 4. What are the components of a framework to evaluate UX of end user program security features?	To determine the suitable security criteria/ methods that can be used to evaluate UX of end user program security features. To determine UX metrics/evaluation criteria can be used to determine the UX of end user program security features. To determine components and requirements of end user program security features' UX and use them to develop the EUPSFUX framework.	From the surveys, literature review, heuristic evaluation and case study. Design science research methodology- stage 3 design and development
Main Research Question: How can a framework be designed to evaluate the user experience (UX) of interacting with end user program security features from a user's perspective?	To determine components and requirements of end user program security features' UX and use them to develop the EUPSFUX framework.	Design science research-methodology- stage 3 design and development

Table 1-1 is a summary of the research questions, objectives and research methods that are employed in the study.

1.7 ETHICAL CLEARANCE

The country under which the study was undertaken does not have a procedure for ethical clearance; however, a written document was signed between the researcher and the security custodians of the case organisation. Despite this, all measures were executed to ensure that the study adheres to all ethical requirements. Survey participants were not required to submit any personal information and participated on a voluntary basis.

1.8 RESEARCH SIGNIFICANCE AND CONTRIBUTION

This research makes a contribution to the body of knowledge by developing a framework for evaluating the user experience of interaction with end user application program security features. The framework can also be used to influence and maintain acceptable UX levels in institutions of higher education by focusing on human factors influencing interaction with technology. Metrics for establishing UX baselines and evaluating the impact of intervention were also developed.

1.9 CHAPTER OUTLINE

There are eight chapters in this thesis. Chapter 1 is an introduction to the thesis, outlining the background to the research, the problem statement, objectives, research questions and methodology plus the scope of the research. In Chapter 2 methods that were used to answer the research questions and to achieve the objective are discussed in detail. Chapters 3 and 4 discuss the theoretical underpinnings of the study. Chapter 3 focuses on information security, usable security, end user program security features, including the metrics and evaluation methods applicable to each, whilst Chapter 4 discusses the human factor of information security, focusing on user experience (UX), user behaviour (UB) and HCI security culture, as well as heuristics and evaluation methods. Chapter 5 presents the case studies conducted in an academic institution using user studies, heuristic evaluation of usability, UX and security in MS Word and Adobe, as well as the findings. In Chapter 6 the framework design process and the resulting framework are presented. Chapter 7 presents the finalisation of the proposed framework and a presentation of contributions. Chapter 8 concludes with reflections, lessons learnt, limitations, recommendations and possible future research. Figure 1-3 is a pictorial representation of the thesis layout.

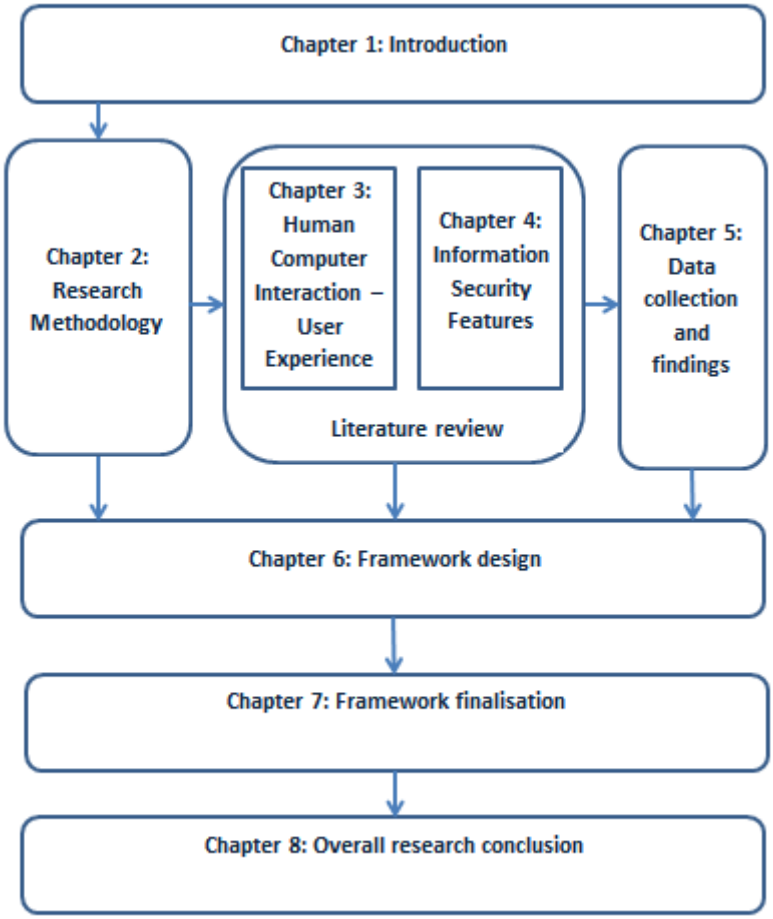
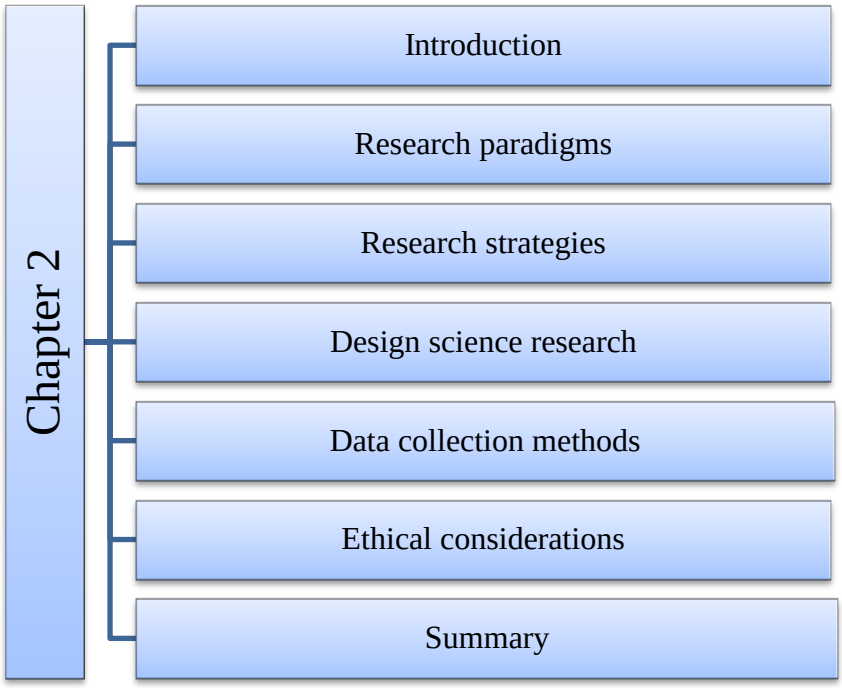


Figure 1-3: Thesis layout

CHAPTER 2: RESEARCH METHODOLOGY

2.1 INTRODUCTION

The first chapter introduced the problem to be addressed in this research. This chapter sets out the methodology that was used to answer the research questions, to collect, analyse and interpret results in order to meet the research objectives. The chapter follows the order presented in the chapter map. Section 2.2 presents the research paradigms and the underlying philosophical assumptions, followed by an overview of research strategies in Section 2.3. In Section 2.4 the design science research paradigm and philosophical assumptions applicable to this thesis are presented; Section 2.5 presents data collection and analysis instruments. Section 2.6 discusses the ethical considerations for this research. Finally, the summary is presented in Section 2.7.



2.2 RESEARCH PARADIGMS AND THE PHILOSOPHICAL ASSUMPTIONS

Paradigms are sets of shared research assumptions or ways of thinking about a phenomenon (Oates, 2012; Denzin & Lincoln, 2005). Researchers have a personal or shared understanding of reality (ontology), ways of exploring knowledge (epistemology), the value of the knowledge (axiology) and procedures for acquiring it (methodology) (Vaishnavi & Kuechler, 2004; Oates, 2012; Denzin & Lincoln, 2005). These four philosophical assumptions help in

describing and adopting the paradigms. The number of research philosophies and paradigms vary from discipline to discipline. There are two paradigms that are generally agreed upon; the positivist and the interpretivist paradigms. Other paradigms, such as critical science, development/ design science, pragmatism, functionalism, radical structuralism and radical humanism also exist (Oates, 2012). When applying the qualitative research choice, usually there are three choices for information systems, namely: critical science, positivism and interpretivism (Bhattacherjee, 2012; Saunders, Lewis, & Thornhill, 2009; Oates, 2012). When it comes to HCI three paradigms are common, namely: traditional science, design science and human factors engineering. Other HCI paradigms include phenomenological matrix and experience-centred design. According to Venable (2011) there are five research paradigms, namely: interpretivist; positivist; theoretical-argumentative; critical, and design science. This research is in the HCI domain and focuses on designing an artefact; as such, design science needs to be considered alongside the two popular paradigms. Table 2-1 presents the Design Science Research (DSR) alongside two popular and generally accepted paradigms.

Table 2-1: Research philosophies and associated reasoning (Oates, 2012; Denzin & Lincoln, 2005; Vaishnavi & Kuechler, 2004)

	Research Paradigm		
Basic Belief	**Positivist**	**Interpretivist**	**Design Science**
Ontology	Single truth, definite, probabilistic, external	Multiple realities, socially constructed, dynamic	Multiple, contextually situated alternative world-states, socio-technologically enabled
Epistemology	Objective, dispassionate, detached observer	Subjective based on researcher-participant interaction, reflexive	Knowledge through building, iterative design, contextual construction, iterative circumscription
Axiology	Hypothesis testing	Exploration	Control, creation, improvement, understanding, artefact utility
Methodology	Observation, statistical, quantitative	Participation, hermeneutical, qualitative, dialectical	Developmental, gauge artefact impact on composite system

Research is an activity that enables the understanding of a phenomenon (Vaishnavi & Kuechler, 2004). With interpretivism the researchers study naturally occurring social events using subjective understanding of the variables involved (Myers & Avison, 2002). On the

other hand, DSR creates part of or the whole phenomenon instead of it occurring naturally; as such, it is a science of the artificial (Simon, 1996). DSR is therefore applicable in designing the solution, as it is used to come with novel and innovative artefacts through an iterative process of building and evaluation with abstraction. Interpretivism was employed in this study. Participants were interviewed for their opinions and the responses were analysed qualitatively and variations were reconciled from the researchers' independent perspectives (Bhattacherjee, 2012; Saunders et al., 2009).

2.2.1 Research Paradigm and Philosophical Assumptions Applicable to this Study

In this thesis an in-depth understanding of a phenomenon in context was sought through an interpretation of population views and these are dynamic as they are influenced by context in time. Ontologically multiple realities in context, which are socially constructed and dynamic, exist depending on end user characteristics; on the organisational security culture as well as on the product in use at any given time. Owing to the nature of this research, positivism will not be considered as it assumes that fixed realities exist that can be measured objectively. DSR and interpretivism offer multiple realities; however, they differ in that interpretivism offers dynamic realities while DSR has multiple static views of reality that are socio-technologically enabled.

From an epistemological point of view, user experience is subjective as it depends on technology and end user interaction.

Methodologically, data is collected and analysed qualitatively in context through surveys. An artefact is built iteratively through reflection.

From an axiological perspective, DSR creates utility and understanding while interpretivism offers contextual understanding.

2.3 RESEARCH STRATEGIES

A research strategy is the complete approach that is used to answer the research question(s) (Oates, 2012; Saunders et al., 2009). There are several research strategies that can be employed and they vary according to the research approach (interpretivism/ positivism) and research choice (quantitative or qualitative) (Sekaran & Bougie, 2009). Case studies, focus groups, ethnography, action research, documents and artefacts (design and creation) are usually employed in qualitative studies that are more inclined to the interpretivist approach (Oates, 2012; Saunders, et al., 2009). On the other hand, experiments, testing, mathematical

modelling and simulation, as well as theorem proving are usually associated with quantitative studies using a positivist approach. Observations and surveys can be used easily with any of the research approaches (Sekaran & Bougie, 2009). This research employed case studies, heuristic evaluation, and surveys, as understanding of a phenomenon was sought. Design and creation was used to design a framework. Having considered the multi-disciplinary nature of the research, case studies and surveys were the natural choice as it has been established that they can be used across disciplines (Creswell, 2013).

The main objective of this research is to design a framework; it incorporates design science research (DSR), also known as design and creation, as it focuses on coming up with artefacts. DSR is a problem-solving strategy aimed at building and evaluating artefacts to address phenomena (Hevner et al., 2004).

The DSR as a strategy is presented in Section 2.4, together with the application thereof in this thesis.

2.4 DESIGN SCIENCE RESEARCH STRATEGY OVERVIEW

Real world problems are usually addressed through innovative artefacts (Simon, 1996). Ellis and Levy (2010) developed a systematic way of identifying a research problem by following the problem based research cycle. When the problem has been identified, solutions are explored and, where necessary, a framework is designed to address the phenomena. The developed framework is applied to the context and evaluated for applicability in a specific domain. To develop a domain-specific framework, it is necessary to follow domain-specific guidelines. DSR is recognised as one of the methodologies applicable to HCI and IS, especially when addressing social problems(Vaishnavi & Kuechler, 2008).

The design science research paradigm comprises the design of original or inventive artefacts and the study of the usage and/or behaviour of such artefacts to enhance and comprehend the behaviour of features of Information Systems. Design science research is an additional way of complementing the positivist and interpretivist philosophies for performing research in Information Systems (IS) (Vaishnavi & Kuechler, 2008). According to Weber (2010), DSR can either be a paradigm or a research approach; however, it can be used in either of the other paradigms as a complement. In this study it is used as a strategy to complement interpretivism. Philosophical paradigms are reflected in the research strategies employed in a study process.

DSR begins with awareness of the problem, followed by a suggestion of a design/ concept, development, and then evaluation, as shown in Figure 2-1. The steps can be iterated until an initial design is developed; then conclusions can be drawn (Vaishnavi & Kuechler, 2004).

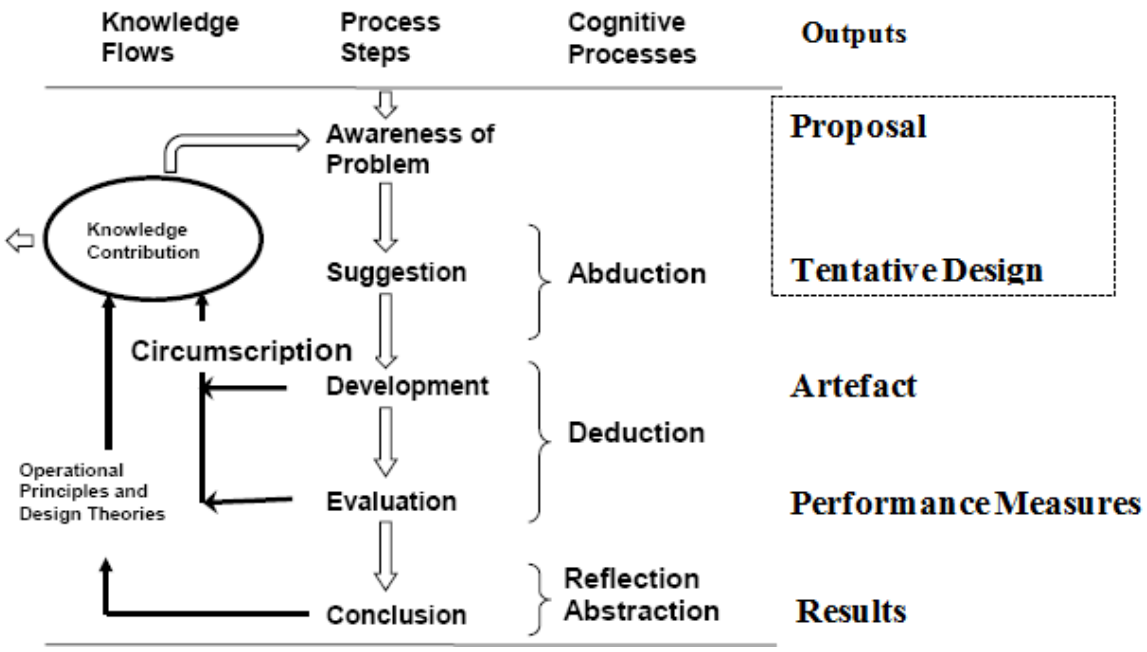


Figure 2-1: DSR Methodology adopted from (Vaishnavi & Kuechler, 2004; Vaishnavi & Kuechler, 2008 p.20)

Each phase has an output linked directly to the products (outputs) as shown in Table 2-2, identified by Vaishnavi & Kuechler (2004). The next section presents DSR research products.

2.4.1 Design Science Research Products

Four commonly agreed on products exist, namely constructs, methods, models and instantiations. According to Vaishnavi and Kuechler (2004), artefacts can be algorithms, human computer interfaces and system design methodologies or languages. Products of DSR are shown in Table 2-2 (Vaishnavi & Kuechler, 2004). Vaishnavi and Kuechler (2004) proposed improved theories, whilst Hevner (2007) proposed phenomena/ new meta-artefacts, as well as experiences.

Table 2-2: Research Outputs of DSR (Vaishnavi & Kuechler, 2004; March & Smith, 1995; Hevner, Ram, March, & Park, 2004)

Phase	Output	Description
1	Phenomena	Real life problem under investigation
2	Constructs	The theoretical terminology of the fields of study (UX & IS) to characterise phenomena. Can form domain/ field of shared knowledge.
3	Models	A set of proposals depicting relationships among constructs
4	Methods	A set of steps taken to finish a goal-specific task – research design
5	Instantiations	The implementation of constructs, models and methods.
6	Better theories	Artefact development, combined with reflection and conceptualisation.

2.4.2 Design Science Research Cognitive Reasoning Processes

There are four cognitive reasoning processes in DSR, namely abduction, deduction, reflection and abstraction. Below are brief descriptions of the processes, based on Vaishnavi and Kuechler (2004):

1. **Abduction** is based on existing knowledge, and the output is a tentative solution design that is termed a suggestion. The suggested solution may be inadequate in solving the research problem.
2. **Deduction** is the process where the suggested solution is implemented and evaluated against theory. The evaluation results will reveal and infer (deduce) the inadequacies of the suggested solution and the outcome will then feed into the suggestion for improvements on the design. There is an iteration of suggesting, developing and implementing until a more suitable solution is achieved.
3. **Reflection** is a creative process where the researcher reflects on the research process and learns from it.
4. **Abstraction** is used in the conclusion to make a contribution to the body of knowledge by developing theories or operational principles.

2.4.3 Design Science Research Methodologies

The conceptual framework design process is guided by the adopted definitions of a conceptual framework, and its components, as well as by the guidelines, methodologies and

processes of DSR presented earlier. Several DSR applicable methodologies, approaches, and strategies exist. In this section three of these are described in detail. Worth noting are those developed by Vaishnavi & Kuechler, 2004; Hevner et al., 2004; Hevner, 2007; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008 and Jabareen, 2009.

Jabareen (2009) presented a conceptual framework development process based on DSR methods and process, placing more emphasis on the problem identification and design phases by breaking down the phase into multiple steps. The three-cycle process by Hevner (2007) consolidates the phases into three steps that are cyclical and interrelated, as presented in Section 2.4.5. With this model a lot of detail on how to conduct the process is not used; hence, it can be complex for IS practitioners to apply to their contexts. Peffers's model offers multiple entry levels into the process. However, as the research is problem based, the entry level will be the first one, and all steps are followed sequentially. Different phases followed by different framework development processes as proposed by different authors, based on Vaishnavi and Kuechler's DSRM process.

Focus is first put on seven DSR guidelines by Hevner, Ram, March, & Park (2004). The guidelines provide best practice principles that form the basis of conducting research in a specific domain. Table 2-3 presents DSR guidelines for problem-based research that are derived from the knowledge and understanding of a problem. The research solution is acquired in the development and application of an artefact.

Table 2-3: Research: DSR guideline adopted from Hevner, et al. (2004)

Guideline	Description
Guideline 1 : Design as an Artefact	DSR creates innovative, purposeful artefacts (construct, a model, a method, or an instantiation)
Guideline 2 : Problem Relevance	Develop domain-specific technology-based solutions to address identified problems.
Guideline 3 : Design Evaluation	To demonstrate rigorously the utility, quality, and efficacy of a design artefact using well-executed evaluation methods.
Guideline 4 : Research Contributions	DSR must deliver clear and verifiable, novel and innovative contributions effectively in the areas of the design artefact, design foundations, and/or design methodologies.
Guideline 5 : Research Rigor	DSR relies upon the application of rigorous methods in both the building and evaluation of the artefact. The artefact must be rigorously defined, formally represented, coherent, and internally consistent.
Guideline 6 : Design as a Search Process	The search for an effective artefact requires using available resources to get desired results while satisfying laws in the problem environment.
Guideline 7 : Communication of Research	DSR must be published effectively both to technology-oriented as well as to management-oriented audiences.

Having presented the guidelines, the next step is to present processes and methods as proposed by the different authors.

2.4.4 Design Science Research Process models by Peffers et al., 2008

The DSR process model by Vaishnavi and Kuechler (2004) is presented in Section 2.4. Peffers et al., (2008) presented a DSR process with seven stages, as depicted in Figure 2-2.

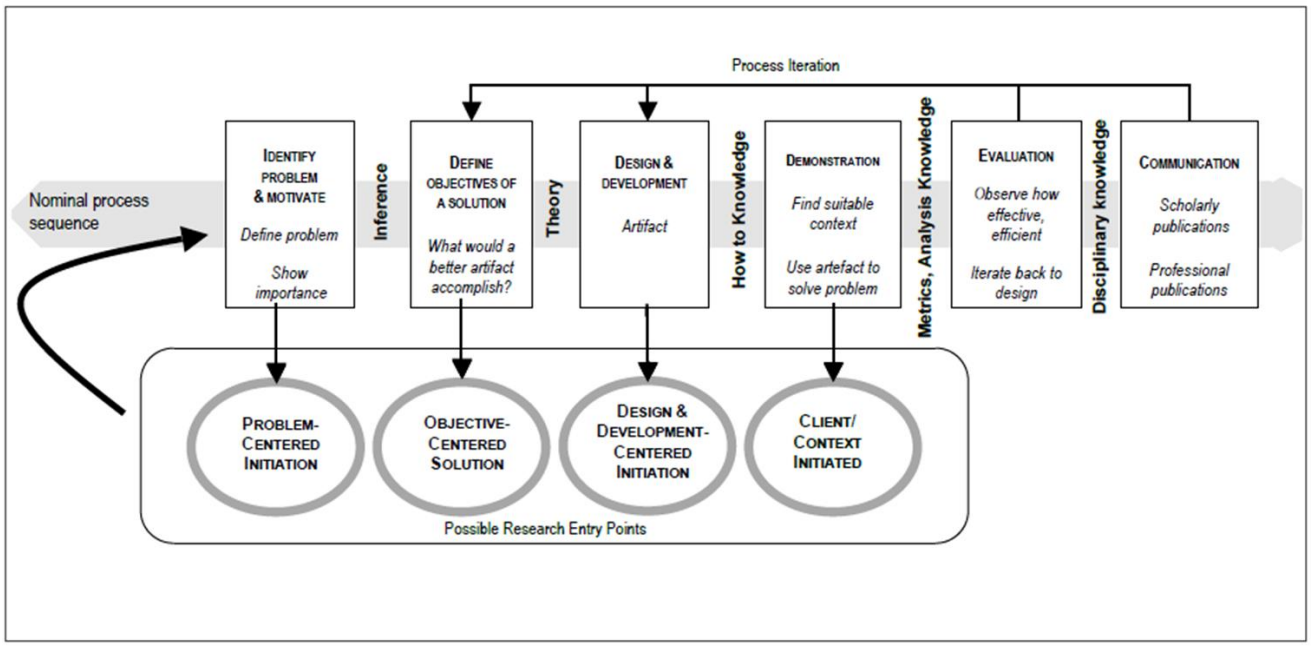


Figure 2-2: DSR Process by Peffers et al. (2008)

The process is a derivative of the design process model proposed by Vaishnavi and Kuechler in 2004. However, the model offers multiple entry points into the artefact design process depending on the type of problem being addressed, unlike the DSRM. Four entry points are offered to cater for problem-centred initiatives, objective-centred solutions, design- and development-centred initiation and client/context initiated. This research follows option1 problem-centred initiation; hence, the process would begin from the start and follow all the steps sequentially. Peffers et al. ,(2008) adds two extra phases and consolidates two into one to Vaishnavi's and Kuechler's five, resulting in six steps in total. Firstly, a design step is included which is about defining the solution objectives based on the problem definition and relevant literature. The suggestion and development phases are consolidated into one step. To demonstrate the applicability of the artefact, a demonstration phase is included before the evaluation and this can be equated to prototyping in software development projects. The final stage is named communication instead of conclusion.

2.4.5 A Three Cycle View of Design Science Research by Hevner, (2007)

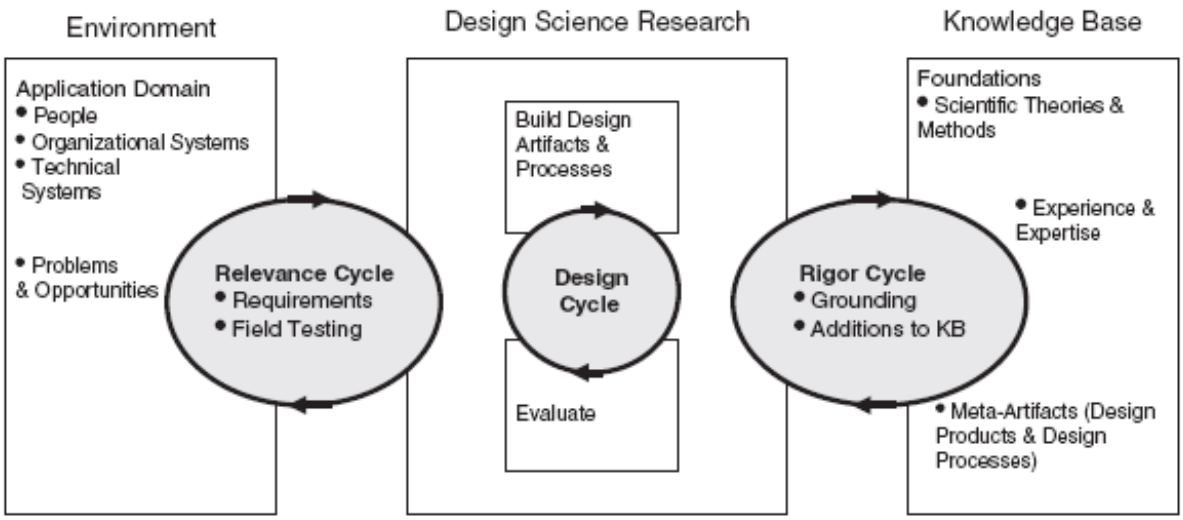


Figure 2-3: Three cycle view of DSR (Hevner, 2007)

According to Hevner (2007), DSR can be viewed as a three cycle process based on the IS research framework by Hevner et al., (2004) as shown in Figure 2-3. The Relevance Cycle connects the research project's contextual environment to design science activities. Thus, the relevance cycle defines the requirements for the research as inputs and the acceptance criteria that are used to evaluate the artefact. The evaluation output is fed into the relevance cycle and the process iterates until a befitting artefact (functionally) has been designed. The Design Cycle at the centre of the rigor and relevance cycles is an iterative process between the main tasks of constructing and assessing the design artefacts and the processes of the research. The Design Cycle iterates between artefact building and its evaluation. Inputs from the Relevance Cycle inform the design and the artefact is evaluated against the knowledge base forming the Rigor Cycle. The Rigor Cycle associates research project design science activities with the knowledge base of scientific foundations, experience, and expertise underpinning the study. Research rigor is demonstrated by the researcher's ability to select and apply appropriate theory and methods skilfully for building and evaluating the artefact.

All the presented DSR methodologies or processes emphasize the importance of evaluation; hence, it is presented in detail in the next section.

2.4.6 Artefacts Evaluation in Design Science Research

DSR invents and develops technologies and always includes an evaluation step to confirm the applicability of the new artefact to its purpose. Hevner et al., (2004) presented five methods

that can be used to evaluate the artefact using the presented criteria. The methods are: observational (using case and field studies), analytical (using static, dynamic and architectural analysis, optimization), experimental (with simulation or controlled experiments), testing (functional or structural) and descriptive (informed argument or scenarios). The methods are presented in Table 2-4.

Table 2-4: DSR evaluation methods (Hevner et al, 2004)

1. Observational	Case Study: Study framework in depth in context of case site
	Field Study: Monitor use of framework in multiple projects
2. Analytical	Static Analysis: Examine structure of the framework for static qualities such as complexity
	Architecture Analysis: Study fit of framework into technical information system architecture
	Optimization: Demonstrate integral optimal properties of framework or provide optimality bounds on its behaviour
	Dynamic Analysis: Study framework in use for dynamic qualities such as performance
3. Experimental	Controlled Experiment: Study framework in a controlled environment for qualities such as usability
	Simulation - Execute framework with synthetic data
4. Testing	Functional (Black Box) Testing: Execute framework interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., understandability) in the framework implementation
5. Descriptive	Informed Argument: Use theoretical information to build a convincing proof on the framework's utility
	Scenarios: Create comprehensive scenarios around the framework to show its utility

Prat, Comyn-Wattiau, and Akoka (2014) presented a hierarchy of general artefact evaluation that focuses on five systems' dimensions and associated criteria. The dimensions are goal (efficacy, validity and generality), environment (consistency with people, organisations and technology), structure (completeness, simplicity, clarity, style, homomorphism, level of detail and consistency), activity (completeness, consistency, accuracy, performance and efficiency)

and evolution (robustness, learning capability). In the next section, framework specific evaluation methods are presented as part of the artefact that is being developed in this study.

2.4.6.1 Framework evaluation methods

Framework should be evaluated for rigor using established evaluation methods (Hevner, Ram, March, & Park, 2004). Criteria include functionality, completeness, consistency, accuracy, performance, reliability, usability, accessibility, aesthetics, entertainment, fitting with organisation, etc. (Oates, 2012; Prat et al., 2014; Hevner et al., 2004).

Table 2-5: Selected framework evaluation criteria per domain

Dimension	**Criteria**	**Demonstrate / Method**
Goal	Validity	Transferability and credibility
		Confirmability
	Efficacy	Achieves the research goal
	Generality	Dependability
Environment Consistency with people's characteristics, roles and capabilities	Utility	Informed argumentation and use case scenarios
	Understandability	
	Ease of use	Peer and expert reviews, case study
	Ethicality	Ethics code of conduct
	Side effects	Case study
Consistency with organisation	Utility Fit with organisation Side effects	Strategies Structure and culture Processes
Consistency with technology	Harnessing of recent technologies	Compare to standards
	Side effects	
Structure	Completeness Simplicity Clarity Style Homomorphism Level of detail Consistency	When it satisfies the requirements and constraints of the problem (complete)
Activity	Completeness Consistency Accuracy Performance Efficiency	
Evolution	Robustness Learning capability	

The evaluation presented will focus on framework evaluation criteria presented in Table 2-5, based on (Hevner et al, 2004; Prat et al., 2014).

Framework evaluation can be practical (using controlled experiments or simulations, dynamic and static analysis or white/back box testing) or theoretical (using observations or descriptions in a field/case study or scenario analysis, and informed argumentation) (Oates, 2012; Hevner, et al., 2004).

To carry out practical evaluation effectively a longitudinal study is ideal as it allows for the artefact to be implemented and evaluated over time for meeting the needs of the situation successfully. However, time was not available to do this, hence alternative approaches were considered. Descriptive theoretical validation using literature argumentation, peer and expert reviews and the use of case scenario analysis were applied.

2.4.7 Quality of the framework

Rigour of the research can be established through the demonstration of the validity and reliability of the research. Care was taken throughout the design phase to ensure that the process demonstrates construct validity, internal validity, external validity, objectivity and reliability. Construct validity requires the researcher to use the correct measures for the concepts being studied. Internal validity demonstrates that certain conditions lead to other conditions and requires the use of multiple pieces of evidence from multiple sources to uncover convergent lines of inquiry. External validity reflects whether or not findings are generalizable beyond the immediate case; the more variations in places, people, and procedures that a case study can withstand and still yield the same findings; the more external validity exists. Techniques such as cross-case examination and within-case examination, along with literature review, help to ensure external validity. Objectivity is the degree of independence from a researcher's bias. Reliability refers to the stability, accuracy, and precision of measurement. The procedures used are well documented and can be repeated with the same results over and over again. (Yin, 2009; Dooley, 2002; Oates, 2012)

2.4.7.1 Validity

Validity is viewed as being either external, where the focus is on whether the research is generalisable to the construct;or internal, which confirms whether there is a relationship between cause and effect and whether it is causal or not.

According to Sekaran and Bougie (2009), there are methods of ensuring the validity of qualitative research, such as:

1. Supporting generalisations by counts of events
2. Ensuring the representativeness of cases and the inclusion of deviant cases
3. In- depth description of the research.
4. Triangulation that ensures confidence in the result by employing different methods/ sources to get the same results. Multiple perspectives should be used to conduct research. Types of triangulation are (Sekaran & Bougie, 2009, pp. 384-5, Yin, 2009, Oates, 2012, pp.37):
    a. Method: several methods for gathering and synthesising data. For data collection interviews, surveys using questionnaires and expert reviews were used.
    b. Strategy: In this study, case study, surveys and design and creation strategies were used to conduct the research.
    c. Data: data is gathered from multiple sources and /or at different times.
    d. Researcher/investigator: several researchers gather/synthesise data.
    e. Theory: employ several theories or perspectives to analyse and report the data.
    f. Environment: varies in environmental factors (time, location) and evaluates the impact of the variation. Oates separates these into space and time.

All these methods were incorporated at different stages of the study. The validity of a questionnaire was assessed on content validity, criterion-related validity and construct validity. Content validity is the degree to which the questions in the questionnaire give sufficient reporting of the phenomena under study. Criterion-related validity, also known as predictive validity, assesses the ability of the questions to make precise estimations by comparing the data to specified criteria. Construct validity refers to the ability of the questions to measure truly the existence of those constructs they were meant to measure (Saunders et al., 2009).

The research paradigm followed in this research is interpretivism; hence, reference is made to how much trust can be placed in the in research. Trustworthiness is the level of trust that can be placed in the research based on the use of valid methods and techniques derived from literature to measure framework components.

1. **External validity** is difficult to demonstrate as multiple realities exist and they depend on variable factors; therefore transferability will be demonstrated. Transferability is the extent to which the research is generalizable to different environments, participants, and time, and depends on the representativeness of the sample studied (Oates, 2012, p. 294). However, environmental aspects such as organisational culture and personal dispositions make it impossible to apply the same process in a different context. Instead, focus is on transferability of the findings to other similar contexts.
2. **Internal validity** is demonstrated by evaluating the credibility of the research. Credibility is the degree to which findings are precise, compare to reality and measure it correctly; however, in interpretivist research there are several created realities; hence, there is no benchmark for testing the results (Oates, 2012, p. 294). Instead, the focus is on the credibility of the research process. Triangulation of methods, strategies and data are used to demonstrate this aspect.

2.4.7.2 Reliability

Reliability ensures that the research process can be followed by other researchers and produce the same results under similar conditions. It can be classified into inter-rater/observer which demonstrates equivalence or parallel forms; or test-retest; these two both test stability and internal consistency which tests homogeneity (Sekaran & Bougie, 2009). The research was done by one researcher; hence, inter-rater/observer reliability is not applicable. The time horizon of the study was cross sectional; no multiple data collection/measures were done, so this rules out test-retest reliability in the study. A single case study was used making it impossible to compare data from a similar content domain, so this rules out parallel forms reliability. In this study internal consistency is demonstrated. A single measurement instrument is distributed to a number of people at the same time to evaluate.

Reliability is usually centred on the repeatability of the study; however, when a social problem is studied it is bound to vary at different times as the influencing conditions evolve. As such, data collected at different times cannot be similar (Oates, 2012, p. 294; Hevner et al., 2004). Moreover, as the researcher's involvement impacts on the outcome, therefore different researchers will produce different results. The dependability is demonstrated instead, as it speaks to the research procedure and data recording which allows an audit to be carried out successfully on the research process (Oates, 2012, p. 294; Saunders et al., 2009).

To demonstrate dependability, the following tools and methods were used:

1. The questionnaire was pre-tested with the comments of seven people, and feedback was used to improve the tool.
2. The questionnaires were self-administered to eliminate the bias to please of the participants answering the question
3. Research methods and strategies are clearly documented in Chapters 2, 5 and 6.

2.4.7.3 Objectivity

According to the Merrian Webster dictionary, objectivity "relates to, or being an object, phenomenon, or condition in the realm of sensible experience independent of individual thought and perceptible by all observers: having reality independent of the mind." (Webster, 2015).

Objectivity cannot be demonstrated in this case because the researcher has personal experiences that can influence the interpretation of the collected data. Moreover, the researcher is a member of the community being studied and interacts with participants often. As such, focus is placed on the demonstrated confirmability of the findings. Given the collected data, summaries and the analysis, another researcher can draw the same conclusions. Another researcher should not necessarily be able to replicate the study, but should be able to assess in detail what was done, why it was done, and how conclusions were deduced (Meyers & Sylvester, 2006).

To demonstrate confirmability, the following tools and methods were used:

1. Clearly outlined methods and processes used for data collection and analysis
2. Use of literature to confirm findings

2.4.8 Design Science Research Strategy Application to this Thesis

The DSR process model used for framework development, in particular to this study, is the DSRM process model of Peffers et al., (2008). The process model involves six phases presented in Section 2.4.4. This research follows the nominal sequentially ordered process structure from activity one to six, as shown in Figure 2-4.

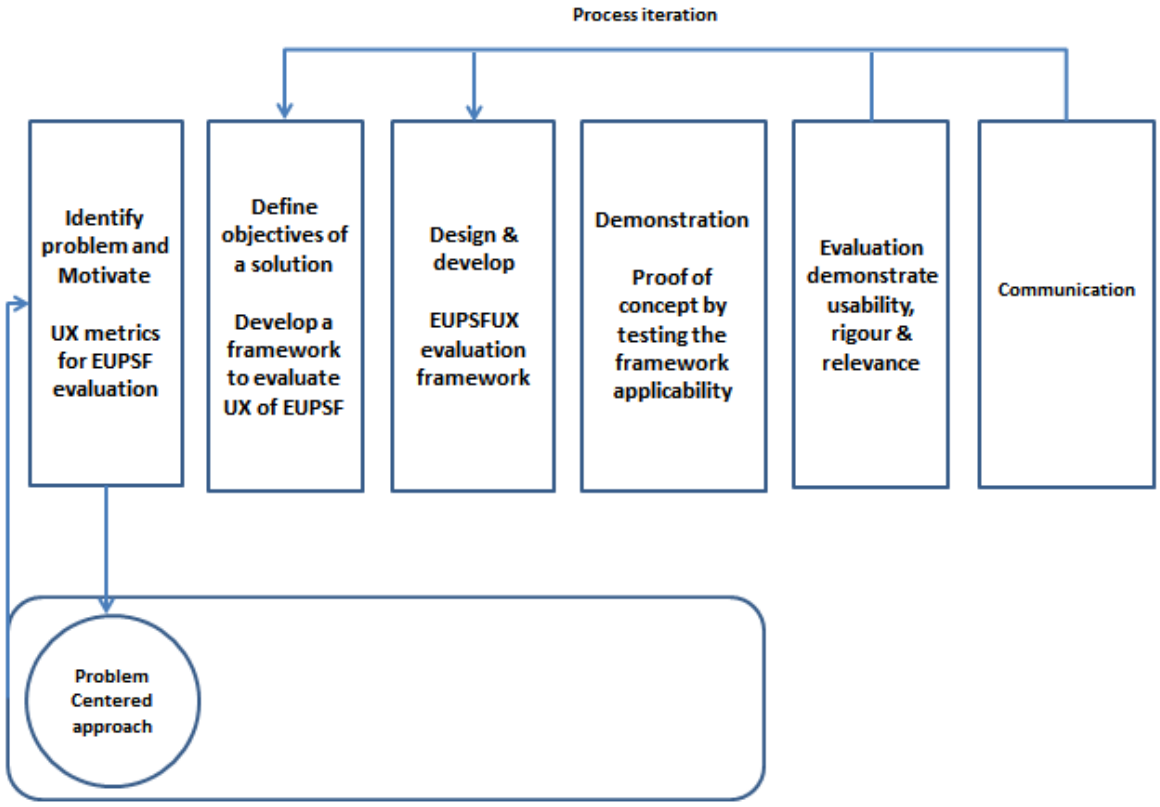


Figure 2-4: DSRM process for the EUPSFUX framework

Each of the activities is summarised in Table 2-6 and the chapters that focus on each activity are shown in column 3. The table presents a general description of each phase. Phase 1 used literature and user studies in a case site to define the problem in line with problem-based research. Phase 2 is derived from literature studies, and findings from user studies in Phase 1. In Phase 3, the theoretical framework is derived from Chapters 1, 3 and 4 and evaluated against case study findings in Chapter 5. The artefact is then developed in Chapter 6. Constructs for the conceptual framework are identified and verified. Phase 4 demonstrates the suitability of the framework through the use of user studies in the case site, the use of case scenarios and validation through literature. In Phase 5, the framework is evaluated through theoretical studies, as well as through expert and peer reviews. After incorporating feedback from the evaluation process iteratively to Phases 2 and 3, the final framework is developed and communicated for public commenting in Phase 6.

Table 2-6: Framework development process

Activity	Description	Associated chapter
Phase 1: Problem identification and motivation	A definite problem as well as the application domain is identified and the value of the proposed solution is motivated.	Chapter 1
Phase 2: Define the objectives of a solution	Objectives of the solution are inferred from the problem definition, user studies and literature. Objectives can be quantitative or qualitative, where a new artefact is created to support solutions to the identified problem.	Chapter 1
Phase 3: Design and development	Identify and design the desired artefact, which is usually one of the DSR outputs presented in Section 2.4.1. The desired functionality, architecture and creation of the actual artefact are typical activities in this stage. Theoretical knowledge will be required as one of the resources plus contectual data collected from end users in the case site.	Chapters 1,2, 3,4,5 and 6
Phase 4 : Demonstration	The process of establishing that the artefact can solve the identified problem effectively. The demonstration can be an experiment, simulation, a case study or proof of concept. This stage requires knowledge of how to use the artefact to solve the problem.	Chapter 3.4,5 and 6
Phase 5: Evaluation	Measures the degree to which the artefact supports the proposed solutions to the identified problem. Successful evaluation requires knowledge of relevant evaluation metrics and analysis techniques. It involves a comparison of the solution objectives to results, artefact demonstration and sometimes to the artefact's functionality, quantitative performance measures, or simulations. The results of this stage can inform the researchers whether it is necessary to iterate back to step 3 to improve the effectiveness of the artefact or to finalise the process in the communication phase.	Chapter 6
Phase 6: Communication	Sharing information with different audiences about the problem, its significance and the artefact's utility, novelty and design rigour.	Chapter 7

The next section will present each phase contextually in detail.

Phase 1: Problem Identification and motivation

Design science research stage 1, in line with problem based research cycle stage 1 and 2, was used to define the problem that will be addressed by the framework. The problem is:

There is a lack of User Experience evaluation criteria to assess the user experience while interacting with embedded security features in end user programs.

Figure 2-5 is a pictorial representation of the problem identification process, which is presented based on the pilot study and literature review.

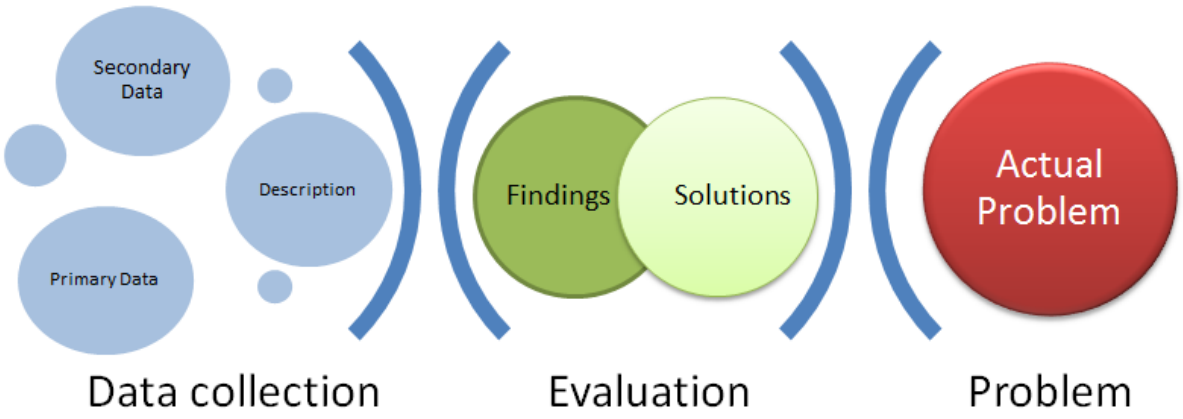


Figure 2-5: Problem identification

End user experience of EUPSF interaction influences the usage of the features as well as the security posture of the organisation. There is a need to identify suitable security and UX evaluation criteria applicable to EUPSF in organisations and implementation guidelines that can enable the implementation and evaluation of their application. A EUPSFUX evaluation framework is thus necessary as it can present the evaluation criteria and the implementation guidelines, as well as the evaluation criteria.

Phase 2: Define the objectives of a solution

To address the identified problem, the following research objectives needed to be achieved by answering specific research questions using DSR in a case study setup. Table 2-7 matched the research objectives of the solution and the corresponding research question that will address the objective.

Table 2-7: Research objective and corresponding questions

Research objective	Research question
Main: To design a framework that can be used to evaluate the user experience of interacting with end user program security features from a user's perspective	How can a framework be designed to evaluate the user experience (UX) of interacting with end user program security features from a user's perspective?
To measure the state of UX with end user program embedded security features.	What are the factors affecting UX with embedded security features in end user programs?
To determine the components and requirements of end user programs' security features' UX and use them to develop the EUPSFUX framework.	What are the components of a framework to evaluate UX of end user program security features?
To determine the suitable security criteria/ methods that can be used to evaluate UX of end user program security features.	What are the suitable usable security evaluation criteria/ methods that can be used to evaluate the usability of end user program security features?
To determine UX metrics/evaluation criteria can be used to determine the UX of end user program security features.	Which UX metrics/ evaluation criteria can be used to determine the UX of end user program security features?

Phase 3: Design and Development

Different key fields and domains established from a preliminary literature review are brought together to define the theoretical framework presented in Figure 2-6. Key domains are human factors, user experience, usable security, user behaviour and information security. To validate the importance of the components of the theoretical framework to the framework, an empirical study conducted is presented in Chapter 5. Based on findings of the case study in Chapter 5, constructs are verified and their components are identified. The components are then related to other components and relationships are modelled. Since the study is focusing on end users, this makes them a key stakeholder, as the framework will be evaluated for addressing their identified problem adequately. Other stakeholders involved are technical experts in the identified fields such as HCI, USec, UX and InfoSec, as well as IT technical support team. This section will be covered in detail in Chapter 6 that addresses the following sub-questions:

What are the factors affecting UX with embedded security features in end user programs?

What are the components of a framework to evaluate UX of end user program security features?

The identified components and relationships are put together to present a conceptual model. An implementation guideline is developed. This section will be covered in detail in Chapter 6, which addresses the main research question:

How can UX factors necessary for end user program security features' UX evaluation be constituted into a framework?

Phase 4: Demonstration

This phase will establish whether or not the EUPSFUX framework can solve the lack of evaluation criteria for UX with EUPSF effectively. The demonstration can be an experiment, a simulation, a case study or proof of concept and requires knowledge of how to use the artefact to solve the problem.

The application of the framework is thus demonstrated in Chapter 6 using theoretical validation, task scenario analysis and literature. According to Hevner et al. (2004), artefacts created in design science research are not often implemented in practice, but they describe innovatively the concepts, practices, practical competences and products which ensure effective and efficient IS use, design, analysis and implementation. In light of this, task scenarios will be modelled and evaluated to demonstrate the applicability of the framework. During the development, as well as the evaluation of the framework, stakeholders were selected purposefully to evaluate the different stages. This section will be covered in detail in Chapters 3, 4 and 5, which address the following sub-questions:

What are the suitable usable security criteria/ methods that can be used to evaluate UX of end user program security features?

Which UX metrics/evaluation criteria can be used to determine the UX of end user program security features?

In Chapter 6 the identified criteria are applied to the framework to evaluate the components.

Phase 5: Framework evaluation

The purpose of this stage is to demonstrate the applicability of the developed framework to the problem domain. Utility, quality and efficacy of the framework is rigorously established using well-implemented evaluation methods (Hevner et al., 2004). The framework is assessed using implicit criteria that were explicitly presented in the literature review (output of the awareness of problem phase). Nonconformities to qualitative anticipations are documented and will be described tentatively. The analysis will explain the framework behaviour and will establish whether or not there is a need for iteration. This section is covered in detail in Chapter 6, which addresses the main research question:

> **How can UX factors necessary for end user program security features' UX evaluation be constituted into a framework?**

Phase 6: Communication (Finalising the framework)

The process, framework and evaluation results will be shared with other researchers and the organisation where the case study took place. This will be detailed in Chapter 7, which is the framework finalisation. Reflection on the study process is provided. Findings from the study are published in peer reviewed conferences and journals.

2.4.9 Cycles of the Design Science Research Process

According to Hevner (2007), there are there cycles to follow: relevance, design and rigor. The relevance cycle comprises problem awareness, which is Phase 1 and 2 of the DSR methodology process, by Peffers et al. (2008). The environment is the Polytechnic of Namibia, and the application domain is characterised by end users, end user programs, end user program security features, organisational systems and UX problems. The second cycle, design, comprises framework design, suggestion, framework application and evaluation; Phases 3 to 5 of the DSR methodology process. The third and last cycle is rigor and it corresponds to Phase 6, communication, of the DSR methodology process. Figure 2-6 shows the iterations between the cycles.

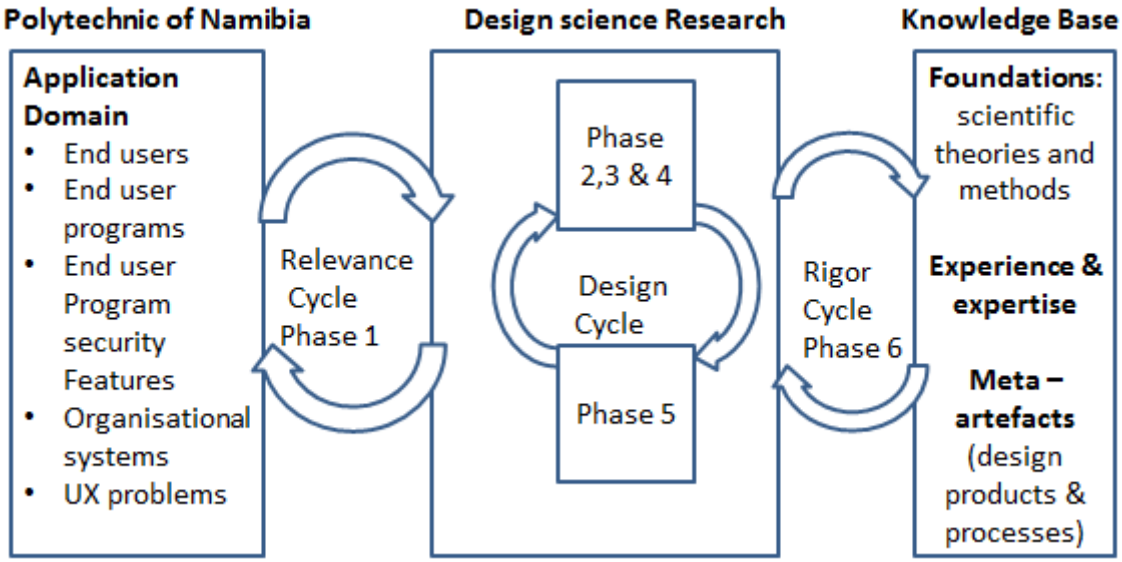


Figure 2-6: DSR cycles applied to thesis

2.4.10 Research Cycles to develop the framework

In this section the research cycles are presented and are linked to research objectives.

1. To measure the state of UX with end user programs' embedded security features.
2. To determine the suitable security criteria/ methods that can be used to evaluate UX of end user program security features.
3. To determine UX metrics/evaluation criteria can be used to determine the UX of end user program security features.
4. To determine the components and requirements of end user programs' security features' UX and use them to develop the EUPSFUX framework

Research cycle 1 is the relevance cycle and it enables the achievement of research objectives 1, 2, 3 and 4. A case study was used to identify and understand the problem based on literature review.

Research cycle 2 is the design cycle and it enables the achievement of research objective 4 and fulfils the main research objective. This process is iterative; the tentative framework is designed, tested and evaluated. The input is then used to refine the framework design. The cycle is repeated until the desired product has been achieved.

Research cycle 3 is the rigor cycle. In this cycle the framework is evaluated for applicability and for meeting the main objective successfully. This is iterated as many times as the framework is redesigned and the output of each iteration process is recorded.

2.5 DATA COLLECTION METHODS

Data collection methods applied in this research are presented in this section, in line with the research strategy and paradigm being implemented. The research uses qualitative, interpretive tools that support induction.

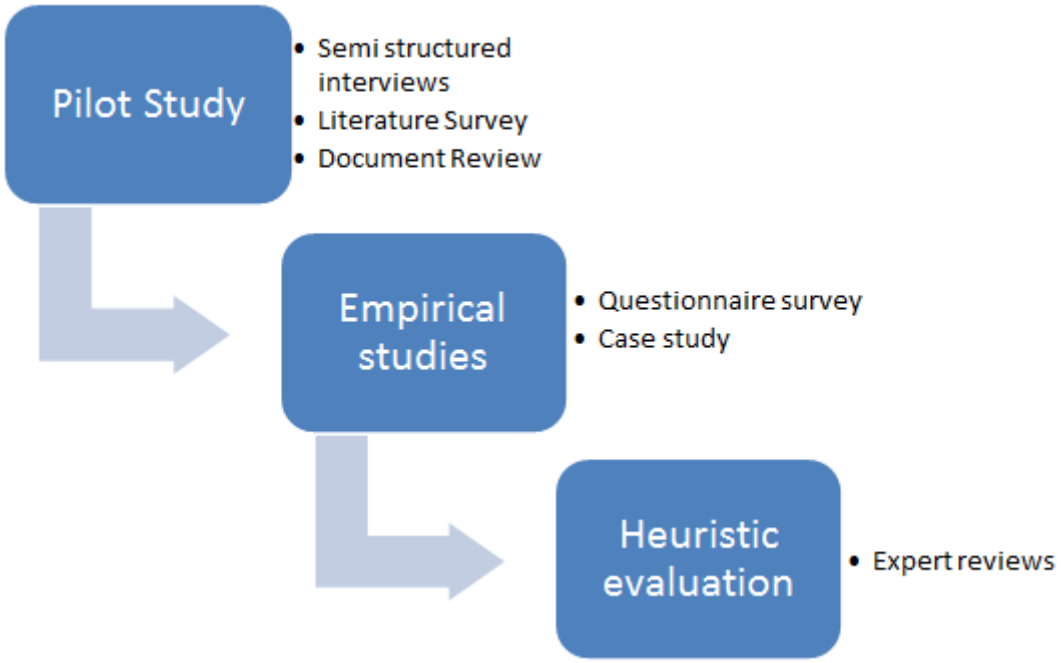


Figure 2-7: Data collection process

Figure 2-7 shows, in summary, how the data collection process evolved. Data collection for qualitative research can use **individual interviews**, focus groups, observations, **questionnaires, documents** and action research (Creswell, 2007; Saunders et al., 2009; Sekaran & Bougie, 2009; Oates, 2012).

Interviews can be unstructured (the interviewer discusses a limited number of topics; they may base interview questions on the interviewee's response); semi-structured or focused interviews (characterised by a number of open-ended questions based on the topic areas that the researcher wants to cover and allows opportunities for both interviewer and interviewee to discuss some topics in depth. It gives the researcher the freedom to guide the interviewee to elaborate on or to follow a new line of inquiry); structured, where the interviewer asks the respondent the same questions in the same way (Creswell, 2007; Saunders et al., 2009; Sekaran & Bougie, 2009).

Focus groups are used to collect information from a group rather than from individuals or when the phenomena under study needs a combined discussion in order to understand the circumstances, behaviour or opinions, as it allows for greater insights to be generated from the group.

Observation takes place in natural settings with the researcher taking lengthy and descriptive notes of what is happening. Action research is when the researcher participates actively in the process, collaborating and making practical changes.

The literature survey: literature is classified as primary, secondary and tertiary.

2.5.1 Case studies

A case study is used to understand phenomena in detail and involves collecting a great deal of information about a specific subject in context using multiple sources of evidence, especially when the boundaries between phenomena and context are not clear (Yin, 2009; Saunders, Lewis, & Thornhill, 2009). The use of case studies is most favourable in situations where the researcher needs to answer the how and why questions without controlling behavioural events, while focusing on contemporary events (Yin, 2009). The phenomena are investigated in their real life context using multiple sources of evidence such as direct observation of events, interviews of individuals participating in the events, documents and artefacts (Yin, 2009).

Case study research is the frequently-used qualitative research method in information systems research, and is appropriate for understanding the interactions between information technology-related innovations and organizational contexts. It is suited for the study of information system implementation, development and use within organisations (Myers & Avison, 2002).

Four types of case study strategies can be chosen using two separate dimensions:

1. Single case vs. multiple case, and

2. Holistic case vs. embedded case (Yin, 2009).

A single case study focuses on a unique, extreme or critical case. On the contrary, a multiple case study strategy investigates phenomena in more than one case. A multiple case study strategy is usually preferable as it allows for the generalisation of findings (Yin, 2009).

The second dimension talks about the unit of analysis. A holistic case is used when the research focuses on one unit as a whole (e.g. an organisation as a whole). In the embedded case, the researcher explores sub-units within one unit (e.g. centres and departments of one organisation).

Dooley (2002) says that case studies can be methodology or strategy. As methodology, they are used to expand and generalise theories analytically rather than to generalise theories statistically (building and testing). As strategy, they hold together multiple methods for the purpose of fulfilling all the phases of research outlined below. However, as methodology they are usually not recommended for studies owing to the following reasons:

1. There is a lack of scientific rigour.
2. They provide little basis for scientific generalisations - multiple cases can be used for generalisations.
3. They are time-consuming and laborious.
4. They are non-experimental; hence, they cannot be used to generate causal relationships (however; they can complement experiments).

Case study researchers such as Yin, (2009) have suggested techniques for organizing and conducting the research successfully, proposing six steps that should be used in order to attain methodological rigour, validity and reliability, namely:

1. Determining and defining the research questions;
2. Selecting the cases and determining data gathering and analysis techniques;
3. Preparing to collect the data;
4. Collecting data in the field;
5. Evaluating and analysing the data;
6. Preparing the report.

On discussing the generalizability from the perspective of interpretive case study research, Walshman (1995) identifies four possible types of generalization: development of concepts, generation of theory, drawing of specific implications, and contribution of rich insight. These allow explanations of particular phenomena derived from empirical interpretive research which may be valuable in other settings and organizations as interpretations of phenomena but which are not wholly predictive for future situations (Walshman, 1995, p. 79).

Research Question 1 is focused on an awareness of the real world problem; case studies with survey strategies were used. Critical literature review was conducted in the different disciplines of the study area, namely InfoSec, HCI security and UX. Once a problem was identified, it became necessary to explore the extent of the problem. Semi-structured interviews gathered preliminary data on the case site. Based on the findings of the pilot semi-structured interviews, a self-administered Internet-mediated questionnaire was developed and deployed using eSurvey pro tool. Questionnaires are good for descriptive or exploratory empirical studies as they allow the researcher to gather large amounts of information that would have been very difficult to achieve with interviews. An exploratory case study was used to evaluate the authenticity of the problem as it allows researchers to gather realistic data of the phenomenon being investigated (Creswell, 2007; Yin, 2009), and this is in line with **Stage 1 and 2** of the design science method. According to Bhattacherjee, (2012), case research is a detailed inquiry of an issue in a case site over a period of time. This method is implemented in social and behavioural scientific research, to gain a detailed contextualised analysis of a social phenomenon within a site (Crinson & Leontowitsch, 2011). Data collection is done using interviews, surveys, literature reviews and heuristic evaluations. This data triangulation ensures that the data is validated. Analysed data was used for artefact building; in this case it is a framework.

In order to understand the end users' perception/attitudes of security, their behaviour and experiences, the survey gathered information on the user's knowledge of security threats to which they are exposed ; their awareness of security policies; their usage of security technologies; their feelings about, experiences with and behaviour towards embedded security features in their application programs.

Both open and closed questions were used as the open questions allow for capturing the feelings or attitudes underlying behaviour, while closed questions allowed respondents to choose an option closely describing them. Closed questions are usually: lists, categories, ranking, rating, quantity and matrix, depending on the type of information required. The questionnaire was pretested prior to full deployment in order to allow for redesign and convergence testing using the initial data. A cover letter explaining the purpose of the survey was broadcast to the population, together with a link to the online survey.

The survey deployment can be:

1. Paper based, which is costly and time-consuming for the users to fill in, or

2. Direct emailing that violates the anonymity of the respondents and presents difficulty in capturing and organising the data, or
3. An anonymous online survey using tools such as Survey monkey, eSurvey Pro.

The choice was an anonymous online survey. The advantages associated with this are:

1. It is fast to deploy;
2. Easy to analyse, and
3. Maintains the anonymity of the participants.

Research questions 2, 3 and 4 involve a critical analysis of usable security and user experience components through literature surveys. USec and UX evaluation criteria for end user program security features were developed by evaluating respective metrics. The outcome was used to come up with a suggestion of a model for evaluating secure UX, which is an output of **Stage 3** of design research DSR process.

The **Main research question** deals with the development of the artefact/framework for secure UX based on the theoretical framework of question 1 and a secure UX evaluation model from question 2.

2.5.2 Data Analysis

Qualitative analysis of qualitative data was used (interpretive text study) to describe the meaning of the data systematically (Schreier, 2012). This involves **data prepation, data reduction, data categorisation; identify patterns and themes, data display** and **the drawing and verifying of conclusions**. These steps are presented in more detail in chapter 5.

The process followed 6 stages, where stage 1 was **preparing** the data for analysis. The data was prepared for analysis by coding the dataset and capturing the responses. Each question was uniquely numbered and each response uniquely coded. Secondly the data was checked for errors, correctness and completeness (**Data cleaning/ reduction**). Thirdly the data was **categorised** and missing values were cleaned up. Numerically coded responses were graphically interpreted and qualitative meanings were inferred from literature. Fourthly qualitative responses were coded per question and **patterns/themes** were deduced. Out of the patterns, themes were generated describing what the participants said. In stage 5 relationships and categories were formed using patterns originating from descriptions, the data was then **displayed.** Finally in stage 6 themes (insights, concepts and conceptual

relationships) were explained using literature allowing for **conclusion** to be drawn and verified.

Data reduction is the procedure of choosing, coding and categorising the data, this was applied to all open ended questions. Data display is the way that the data is presented after the reduction process using charts, matrices, graphs, drawings and frequently used words (Sekaran & Bougie, 2009; Saunders et al., 2009). Initially, the study area was unambiguously described in the context of the case, the objectives and the actions to be taken (Dey, 2005). The context, in this case, is shaped by organisational security culture and support mechanisms in place. Thus, policing and adherence to policies plus security awareness was looked at. The process involves gathering data and analysing it. The gathered data is classified according to exhibited patterns or characteristics for effective analysis (Open coding) (Saunders et al., 2009). The classification was based on research aims/ objectives presented in research questions. Categories were derived from the collected data using frequently used phrases and terms. After classification connections were established among different categories (axial coding). The categories formed the concepts/variables for conceptual framework formulation and the relationships formulated the connections. Inductive propositions that emerged were tested on the data to identify other possible relationships.

The analysis of free-flowing text includes: (1) word based analysis such as key-words-in-context (KWIC), word counts, semantic network analysis; and (2) code-based techniques such as grounded theory, schema analysis, analytic induction, classic content analysis, content dictionaries, and ethnographic decision-making (Ryan & Bernard, 2000). Analysis depends on whether an inductive or deductive research approach was used. Inductive analytical procedures include data display and analysis; template analysis, analytic induction; grounded theory; discourse analysis and narrative analysis (Sekaran & Bougie, 2009). In this research analytic induction was adopted as it allows intensive analysis to establish the underlying cause of a phenomenon. Data was analysed for patterns (themes), and meanings were inferred logically using literature to eliminate bias from the researcher to affect the findings. Description, contextualisation, classification processing and linking were adopted.

2.6 ETHICAL CONSIDERATIONS

2.6.1 Ethical consent

The objectives of the study were presented to the respondents, who made an informed choice to participate voluntarily in the survey.

2.6.2 Anonymity and confidentiality

The users were kept anonymous and everything was done online. The only links that may exist were public IP addresses of the organisation under study. These will not trace the source because Network Address Translation (NAT) is implemented for Internet access. Findings were treated in a confidential manner ensuring that, upon reporting or publishing, no link can be made to the population studied. No personal information was gathered; therefore the privacy of participants was not violated.

2.7 SUMMARY

Chapter 2 described the methodology used to design this research. A discussion of the research paradigm applied in this research and the rationale for the researcher's choices is also included. The population and participants, the data collection tools, data collection plan, and data analysis plans was incorporated. The researcher discussed framework evaluation and ethical considerations in reference to the current research study.

The next two chapters will present background literature on HCI and Information security.

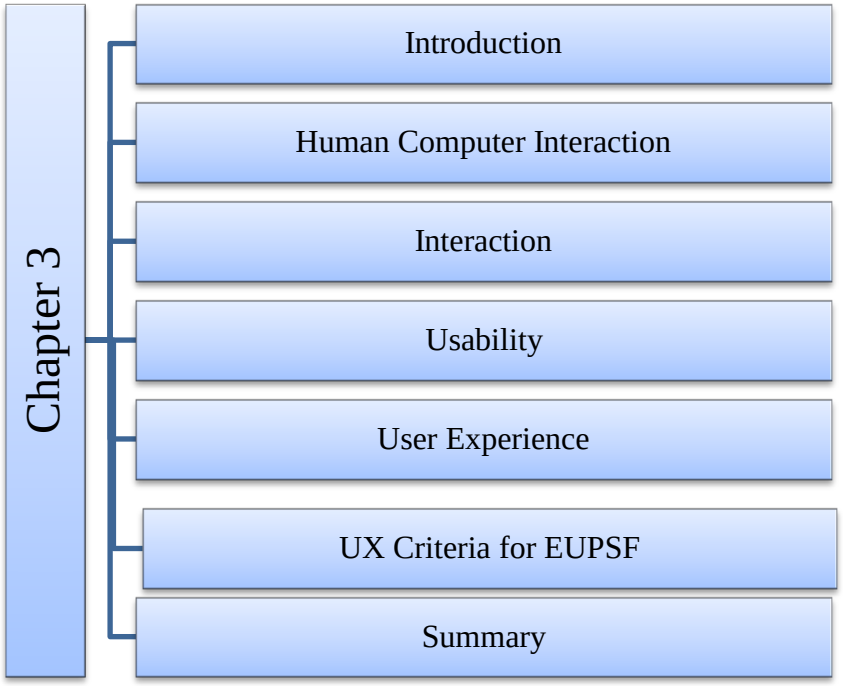
CHAPTER 3: HUMAN COMPUTER INTERACTION - USER EXPERIENCE

3.1 INTRODUCTION

This chapter focuses on the area of Human and Computer Interaction (HCI), a field that deals with User Experience, Usability, Interaction design (known as user centred design UCD) and User Behaviour (UB) disciplines. These disciplines will be used to develop UX with USec evaluation criteria. Models, frameworks and methodologies directly related to the study will be presented. Firstly, the chapter will outline what HCI is, then interaction, usability, UX and finally, user behaviour. At the end of the chapter, the following research question is answered:

Which UX metrics/evaluation criteria can be used to determine the UX of end user program security features?

The content will be presented following the structure presented in the chapter map.



3.2 HUMAN COMPUTER INTERACTION

Human-computer interaction is concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them (Hewett, et al., 1992, p. 5). The human, in this case, will be the end user (EU) of an application program; the computer is any device that has an end user application program (EUP) installed on it; and interaction is the engagement of the EU with the EUP via an interface. HCI encompasses multiple disciplines such as: Computer Science (CS), Cognitive Psychology (CP), Sociology and Anthropology (SA) and Industry Design (ID). The roots of HCI are traced to the fields of Computer Graphics (Art), Operating Systems, Human Factors, Ergonomics, Industrial Engineering, Cognitive Psychology, Linguistics, Philosophy, Artificial Intelligence and the systems part of CS (Hewett, et al., 1992, p.8; Carroll, 2014). The adopted definition helps us to define our study domain that covers Computer Science, Cognitive Psychology, UX and Industry Design. Figure 3-1 shows how the chosen domains interconnect into HCI.

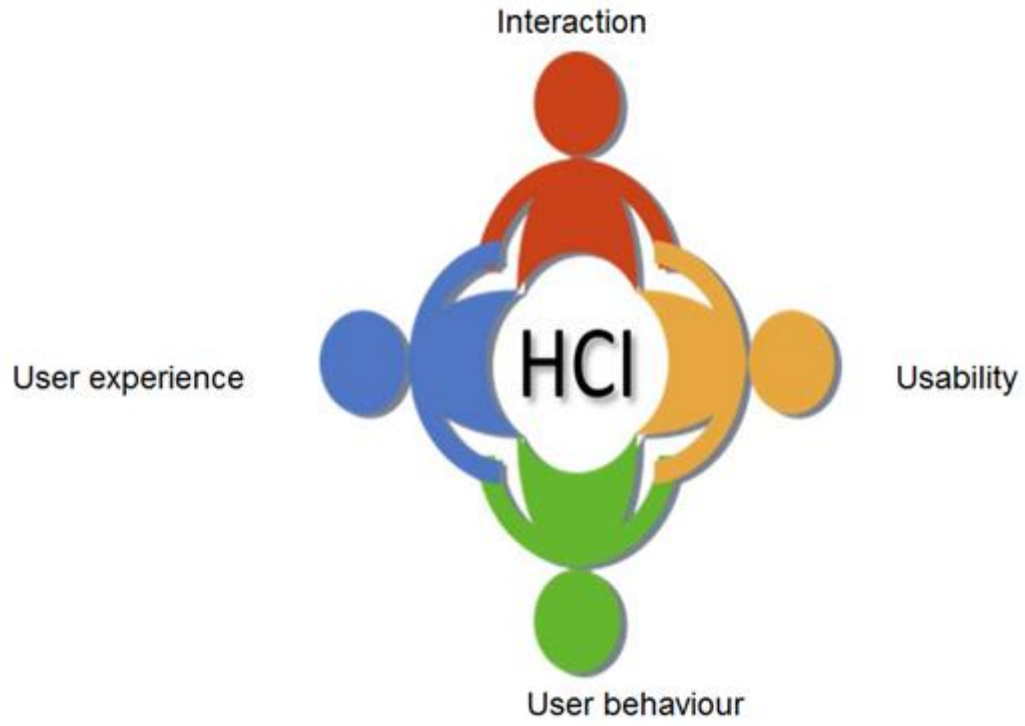


Figure 3-1: Disciplines of the HCI field modification of (Klemmer, 2012)

There are five key aspects to HCI: Nature of HCI (N), Use and context of computers (U), Human Characteristics (H), Computer Systems and Interfaces architecture (C), and

Development process (D).All are applied to Project Presentation and examinations (P) (Hewett, et al., 1992) (Hewett, et al., SIGCHI, 1992).

The nature of HCI focuses on models and frameworks of HCI applicable to UX. The use and context of a computer focuses on human work and application areas. The user has a context or job where the computer and hence the application programs are used. The context determines the interaction type and, as such, can influence how the user behaves. As such, it speaks to the user experience, user behaviour and interaction disciplines of HCI. Human characteristics focuses on dialogue/communication success that depends on the end user's ability to understand the language used during interaction with technology. It covers the user experience, user behaviour and interaction disciplines of HCI Computer systems; and interfaces architecture focuses on dialogue techniques presented to the user and their influence on UX with technology (security features) interaction. This affects the interaction and user experience disciples on HCI.

The development process focuses on design and evaluation techniques. Interaction design determines the usability of a product (security feature) and, therefore, the UX of such use. Appropriate and relevant evaluation tools can be used to ensure that interaction design achieves successful usability; hence, according the user a good UX

In summary, UX is a focus of all five aspects. The nature of HCI (N) which focuses only on UX and interaction are common elements for the key aspects use and context of computers (U), human characteristics (H), context (C) and development process (D). Furthermore, U and H also have UB in common, while D focuses on usability.

From the summary there are two distinct focus areas:

1. Human characteristics, use and context of computers
2. Development process

This research will focus on the first focus area: human characteristics, use and context of computers. It is clear that, in order to address UB, there is need to be aware of user experience of interaction with a particular technology in use and context. Similarly, to address usability issues in technology development, awareness of user experience with technology is important. Technology communicates with users in a way that appeals or frustrates users depending on their human characteristics, which in turn results in an experience.

Focus question:

What are the user experiences with technology (security features) in the case site?

The following sections will present the four aspects of HCI, starting with interaction, then usability, and finally, user experience. User behaviour is a broad subject that needs to be focused on holistically; hence, it will not be discussed.

3.3 INTERACTION

3.3.1 Interaction Design

This is a field surrounded by a cascade of other disciplines such as HCI, UX, industrial design, human factors, architecture, visual and sound design. Lowgren (2014) defines Interaction Design (ID) as a designer action on digital things to characterise them for people's use. The design is characterised by: altering circumstances by shaping and implementing artefacts; exploring probable prospects; outlining the "problem" simultaneously with making potential "solutions; discerning by drafting and other tangible illustrations; speaking to instrumental, technical, aesthetical and ethical aspects all the way. ID varies from traditional designers (product centred) of ICT products who focused on what the product should require, and only delivered on the desired functionality without consideration of human emotions (Lowgren, 2014). Forlizzi and Ford (2000), proposed an early framework for interaction design that can be used to understand the UX which products evoke in end users. The framework has four components describing dimensions of experience, namely: sub-consciousness (no effort to think), cognition (effort to think), narrative (formal or procedural), and storytelling. It is important for designers to have an understanding of the experiences they are designing for and the factors affecting them in order for them to create the right product experience. The framework of Forlizzi and Ford (2000), conforms to the definition of ID in that it focuses on the user perspective of technology; however, it does not prescribe how designers can use this knowledge to come up with a UX centred product. Later Forlizzi and Battarbee (2004) developed a framework for UX, related to the design of interactive systems. The framework informs the designing experience for interactive systems as it focuses on user product interaction and the resultant user experience. As research in the field progresses, Saffer (2010) offers a design strategy consisting of four user product interaction design stages: framing the problem; determining differentiators; visualization and visioning and project planning. Each aims to ensure that products are designed for user interaction. The ISO standard provides guidelines for coming up with interactive software

products. ISO Draft International Standard (D(S) 1307 (1997) is used for designing user centred interactive systems. According to Saffer (2010), there are four approaches to ID, namely **systems design**, **activity centred design**, **genius design** and **user centred design**. Clearly ID is about the user, creating the right user experience and considering user aspects throughout the interaction design process. To capture the nature of ID Saffer (2010) defines three key views to successful ID, namely **technology-centred, behaviourist and social interaction design** views. These views allow for context to be considered when designing solutions for given circumstances. Shneiderman and Plaisant (2005, pp. 74-5) provide eight golden rules (principles) of Interface Design to guide good interaction design especially for mobile, desktop, or web designers. The rules are: **strive for consistency; enable frequent users to use shortcuts; offer informative feedback; design dialog to yield closure; offer simple error handling; permit easy reversal of actions; support internal locus of control; and reduce short-term memory load**. So much has been said about designing for interaction; however, most programs used on computers are mass-produced. This means that they take limited cognisance of the context in which the interaction will take place. The next section will focus on designing product for usability and user experience through user involvement: user centred design (UCD).

3.3.2 User-Centred Design/Human Centred Design

UCD focuses on users and their tasks at the concept of the product design process through user involvement in the design process. Primarily, it should assist designers and developers to comprehend the needs of the people who will use the resultant products (Forlizzi & Battarbee, 2004). UCD aims to design highly usable products. According to ISO 13407 (1999), "Human-centred design is an approach to interactive system development that focuses specifically on making systems usable." This is possible through the application of human factors/ergonomics and usability knowledge and techniques to the user-centric design.

ISO 13407 is a best practice standard on user-centred design, making available guidance on design activities throughout the life cycle of the interactive products. The standard aims to ensure that the needs of all stakeholders are considered during the development and use of interactive systems. Other standards are also developed to address interaction, such as ISO/IEC10741-1, ISO 9241- 10,12,13,14,15,16,17 and ISO/IEC 11581.

The ISO standard on Human-centred design for interactive systems ISO 9241-210 (2010) presents six user centred design principles:

1. Clear user tasks and environments understanding should be the basis.
2. User's involvement throughout design and development.
3. User-centred evaluation drives and refines the product design.
4. Iterative process.
5. The whole user experience is addressed by the design.
6. Design team is composed of multidisciplinary skills and perspectives.

Focus is placed on principles and four activities of UCD, namely plan (identify need and specify context), analyse (specify requirements), design solutions and test (evaluate design and refine), shown in Figure 3-2.

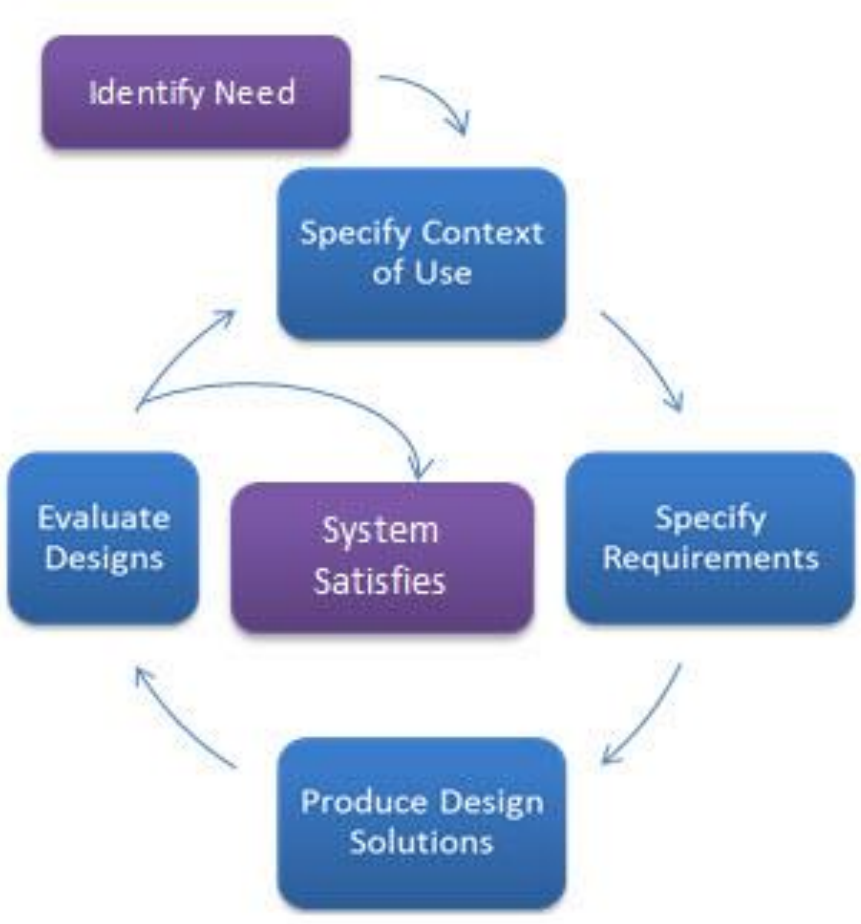


Figure 3-2: UCD activities (www.usability.gov)

There are a number of tools that are used in the evaluation of user-centred design, mainly: personas, scenarios, and essential use cases. Scenarios and use cases will be applied in Chapter 6 to evaluate the research product that is developed from a user perspective

(requirements specification and testing) in line with Phase 4 of the framework development process.

Studies conducted by Cranor and Garfinkel (2005), show that it is possible to realign security and usability with careful attention to UCD principles, and to make security usable. However, it important to note that UCD may result in products that are too specific for more general use; hence, they will not be easily transferable to other environments (Abras, Maloney-Krichmar, & Preece, 2005). In the light of these, how can designers ensure human Computer Interaction Security (HCISec)? The next section presents HCISec.

3.3.3 Human computer interaction security (HCISec)

HCISec aims to improve the usability of security features in end user programs. HCISec focuses on the design, evaluation and implementation of interactive secure systems.

"HCISec is the study of interaction between humans and computers, or human–computer interaction, specifically as it pertains to information security. Its aim is to improve the usability of security features in end user applications" (HCISecAdmin, 2009). According to Johnston, Eloff, & Labuschagne (2003), human computer interaction security (HCI-S) ensures that the security features of a graphical user interface can be more intuitive and user friendly to reduce the chances of users making mistakes or bypassing the security feature. These definitions will guide the literature review of HCISec.

Literature has shown that it is a necessity to improve the usability of security features as a way of ensuring that end users can interact with them as intended by designers (Flechais, Mascolo, & Sasse, 2007; Furnell et al., 2005; Whitten & Tygar, 2005). To address some of the concerns, Garfinkel (2005) developed six principles for aligning security and usability (**i.e. least surprise, good security now, standardised security policies, consistent meaningful vocabulary, consistent controls and placement, no external burden**). Concerns about secure interaction and the usability of security features shift the focus to user-centred design principles as a way of ensuring usability.

Designers focus on both the technical and non-technical aspects that appeal to the user's pragmatic and hedonic expectations while they interact with EUP. User-centred design of secure interaction ensures that the usability principles are incorporated. Yee (2002) established ten principles for designing security from a user-centred point of view, focusing on user interaction design in secure systems. The principles are: **path of least resistance,**

appropriate boundaries, explicit authority, visibility, revocability, expected ability, trusted path, identifiability, expressiveness and clarity. Products meeting these criteria are considered to be adhering to user-centred design. End user program designs follow these design principles and focus on giving the user a memorable experience. For instance, since Office XP, Microsoft has incorporated security controls in their applications to reduce attacks and to improve user experience with the program (Microsoft, 2013). In order for security to be realised, the security controls must be usable. The next section will focus on the usability field of HCI.

3.4 USABILITY

Both UCD and HCISec aim at improving the usability of products. in particular security features. Human error is identified as major cause of security breaches, especially because the system designs are not usable (Furnell et al., 2005; Whitten & Tygar, 2005). Unusable security systems encourage users to make mistakes which compromise security (Flechais et al., 2007). Usability is the degree to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified environment of use (ISO 9241-11, 1998). Usable products are characterised by task efficiency and effectiveness plus user satisfaction. The focus is on what the users want to do with the product/feature (goals) and whether they can do it with little effort and without committing a lot of time. The expertise of the user plays an important role in determining the overall product usability.

Usability is also defined as "the *extent to which an end user is able to carry out required tasks successfully, and without difficulty, using the computer application system"* (Ravden and Johnson, 1989). Since security is designed as a stand-alone tool or embedded within other programs, it is important that it is easy to use and does what the user expects. UCD principles aim at ensuring that the product is usable, when applied to information security, UCD can ensure the design of usable security. According to Ross (2008), "Usability is one of the most important yet hardest design problems in many secure systems. It was long neglected as having less tech glamour than operating systems or cryptographic algorithms yet most real attacks target the user". Poor usability is defined by Whitman and Mattord (2011); Furnell (2005) as the choice taken by end users when confronted to choose the official way of doing a job and the easier unofficial way; they will always prefer the easier one. They propose providing the right way, which is secure only as a solution. Integration of security, usability, training and awareness plus solid controls contribute to system security, while

allowing users to default to easier perceivably usable options will result in compromised security.

This far, literature has shown that it is a necessity to improve security features as a way of ensuring that end users can interact with them as intended by designers (Flechais et al., 2007; Furnell et al., 2005; Whitten & Tygar, 2005). In his research, Furnell (2005) found out that simple is not necessarily secure. Can security and usability be harmonised?

Users need to be impressed or attracted to the features in order for them to make use of the features. Over the years research has focused on improving security design in application design; however, the security features prove not to be usable to the end user. A lot of research is being conducted in the area of usability engineering, a discipline that ensures that a developed software product is usable. Usable is a measure of how an end user can use the program to do their work effectively and efficiently; however, security is not the primary goal of end user programs.

Based on the different approaches that the various authors use to tackle the issue of usability it can be observed that the human component of security is complex and therefore requires special attention to handle it. Usability can be viewed from the designer's (product objectives) and the user's (user needs) point of view.

A user has needs when a program is used, and therefore expects a perceived output; however, when the product is designed, there is an objective to fulfil. Usability can be viewed from the user product perspective; user, product and context perspective; or user, product, context and designer perspective (Hassenzahl, 2004). The objective in most cases does not coincide with the user's needs.

From the designer's point of view, a product is usable if users follow the guidelines as stipulated by the designer. However, because the users have their own characteristics they perceive the product differently and, as such, have their own varying encounters of interaction. Figure 3-3 shows how the designer and end user perspective vary and the impact on the contextual consequences of the interaction (Hassenzahl, 2004).

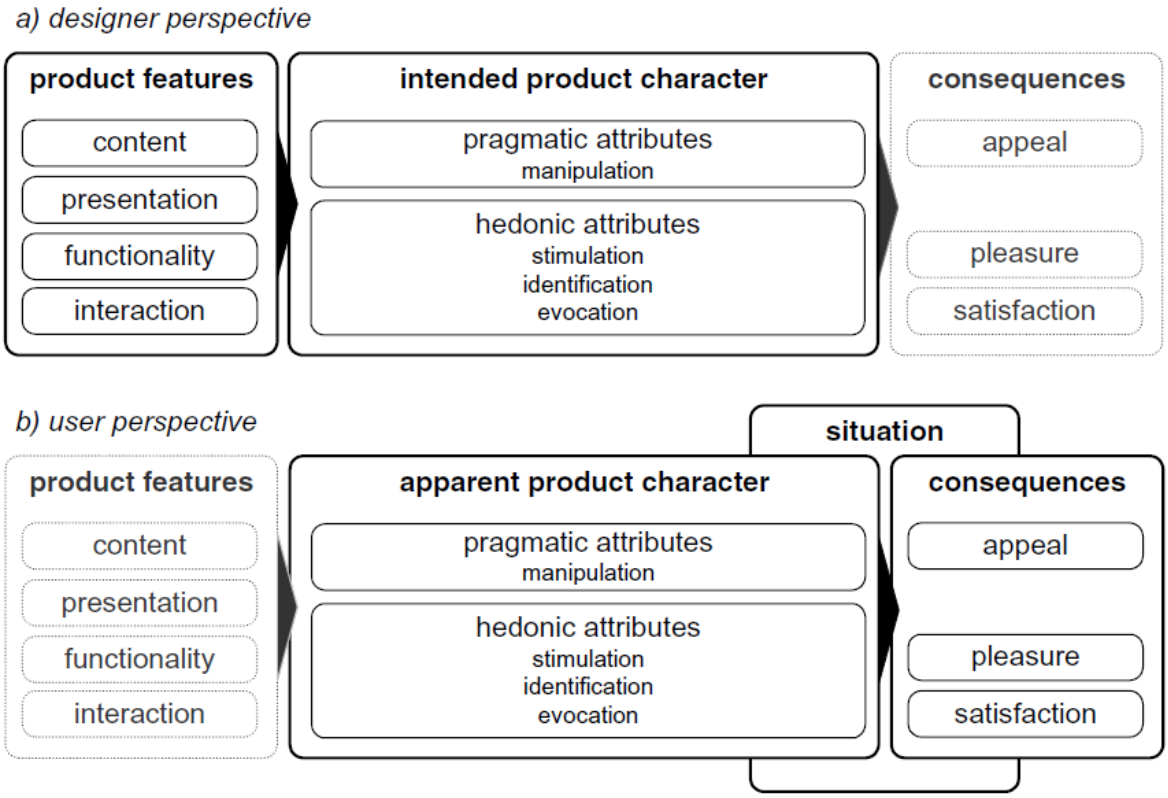


Figure 3-3: Elements of the model of interaction from the designer and user perspectives (Hassenzahl, 2004)

To achieve security usability, models, frameworks and guidelines have been developed. The next section will present these guidelines.

3.4.1 Security Usability guidelines:

Various authors in the field have presented guidelines for USec; among them are those summarised in the following paragraphs. The guidelines were designed for USec designers, so that the designed products can exhibit the desired usability attributes/ characteristics presented earlier.

Usability guidelines for GUIs include Shneiderman's and Plaisant's (2005) eight golden rules for interface design and Nielsen's (1994) heuristics for successful human computer interaction. These should guide the design of interactive security features, which if applied, can ensure user-centred security features. The next paragraphs present USec authors and their respective guidelines.

Whitten and Tygar (2003) presented four attributes of USec in their definition as users: reliably aware of the security task they need to perform; are able to figure out how to perform

those tasks successfully; do not make dangerous errors; are comfortable with the interface to continue using it.

Johnston, Eloff, and Labuschagne (2003) present six criteria for successful security of HCI (HCI-Sec) as: **convey available feature; visibility of system status; learnability; aesthetic and minimalist design; detailed and helpful error messages; satisfaction**. These can be used for interaction design of security features for users.

The six principles for aligning security and usability are: least surprise; good security now; standardised security policies; consistent meaningful vocabulary; consistent controls and placement; no external burden Garfinkel (2005).

Katsabas, Furnell, and Dowland (2005) proposed ten preliminary guidelines for USEC and applied them to ten EUP including MS Word and Firefox. The guidelines are: visible system state and security functions; security should be easily used; suitable for advanced as well as first time users; avoid heavy use of technical vocabulary or advanced terms; handle errors appropriately; allow customization without risk to be trapped; easy to set up security settings; suitable help and documentation for the available security; make the user feel protected; and security should not reduce performance.

Herzog and Shahmehri (2007) presented design guidelines for applications that set a security policy. "Security policy is a set of practices that regulate how an organisation manages, protects, and assigns resources to achieve its security objectives' (Tipton & Krause, 2007, p. 476). The guidelines are as follows: visible not intrusive security; encourage learning; give chance to revise hasty decisions; runtime rather than off-line; enforce least privilege; what has happened, how bad is it? What to do now? Spend time on icons; test and test more?

Yee's (2002) ten principles/ goals of secure interaction design are presented in the security usage section (4.8.1) of the next chapter. In summary they are: path of least resistance; appropriate boundaries; explicit authorisation; visibility; revocability; expected ability; trusted path; identifiability; expressiveness and clarity.

Nielsen's (1994) ten heuristics for successful HCI are presented in Section 3.4.2.5. Briefly they are: visibility of system status; match between system and real world; user control and freedom; consistency and standards; error prevention; recognition rather than recall; flexibility and efficiency of use; aesthetic and minimalist design; help users recognise, diagnose and recover from errors; help and documentation.

So much has been invested in advising designers on how to design user centred security. This guideline will be used to identify usable security criteria. The next section presents user-centred security.

3.4.2 Usable security

Zurko and Simon (1996) defined user-centred security as "security models, mechanisms, systems, or software" that has usability as a main focus, not the design process and testing. Social, technical and production aspects were identified as key areas that can be used to address usable security issues through principles such as safe staging security user interfaces (Whitten & Tygar, 2003; Zurko, 2005). Human computer interaction share a number of commonalities such as evaluation methods, as both can be evaluated in a lab or in actual use through user studies and expert evaluations. For both, validity depends on user-product interaction to demonstrate utility (Zurko, 2005). Section 3.4.2.1 presents security usability problems.

3.4.2.1 Security usability problems

Standards such as common criteria (ISO/IEC 15408) are developed to certify whether a system is technically secure or not; however, there are other problems that arise from the interaction design. As such, security problems are classified according to whether they are: security critical (technical) usability problems or security- non critical (interaction) usability problems (Kaiser & Reichenbach, 2002). Most end user programs are checked and certified for technical issues; hence, for the purpose of this study focus is on the interaction issues. However, the core business of the applications is not security and for any program user who is a security novice challenges are also bound to be encountered with understanding the security. The combination of these two issues presents the user with security critical usability problems. The problems can be due to lack of knowledge regardless of security expertise; hence, there is the need to investigate in context. The next section presents the usable security paradox.

3.4.2.2 Usable Security paradox

Cranor and Garfinkel (2005) identified that realigning security and usability with careful attention to user centered design principles, security and usability can be synergetic. A similar view is shared by many other researchers, including Flechais et al., (2007). Yee (2002) attest to the same view and says "a system that is more secure is more controllable, more reliable and hence more usable"; however, others feel that the two fields are inversely

dependent; improving one will compromise the other. Hertzum, Jørgensen, and Nørgaard (2004) say that usability improvements compromise security and security improvement compromises usability.

In as much as conventional literature cites users as the weak link in Information Security (Siponen, 2006; Sasse 2005; Whitten & Tygar, 2003), some current studies pose evidence that shows the contrary. In business users were found to improve information systems security risk management when they were involved in the prioritization, analysis, design, implementation, testing, and monitoring of user-related security controls within business practices. In fact, user involvement increases organizational awareness of security risks and controls within business processes, resulting in more effective security control development and performance (Spears & Bark. , 2010)

Johnson & Goetz (2007) documented the concerns of security experts at several Fortune 500 companies. They reported that customers expect security to be usable and demonstrably effective.

An international USec research workshop held in Washington DC in 2009 identified the challenges to advancing security and usability research as:

1. Inconsistent terminology and definitions, including terms such as usable security or privacy;
2. Limited data access - the need for more and better empirical data; and
3. Scarceness of expertise and un- familiarity with each other's work—many are working in the field but in distinct and separate disciplines that don't share information.

Moreover, Muller (2006), and Kaiser and Reichenbachm (2002), categorise security and usability issues (problems) as follows:

1. Usability issues do not compromise the security of the system (usability non-critical security)
2. Usability issues that can place security at risk, regardless of the user type.
3. Security critical usability problems - Usability issues owing to user's security awareness
4. Security critical usability problems – User-independent security problems

This research focuses on the third category of security problem in security applications: usability issues owing to user's security awareness.

As if inherent usability issues are not complex enough for users, security features which users can use to make security related decisions, differ from application to application, according to Herzog and Shahmehri (2007). Coupled with the following factors, this has led to emergence of the HCISec field:

1. There is a misalignment between user goals, expectations and security features (Sieger, et al., 2011; Krieger, 2009; Herzog & Shahmehri, 2007). Security is hardly a user's primary concern (No-one buys applications to use the security. (Vacca, 2009))
2. Security features are displayed on fewer occasions, and when these are displayed, the user feels that these features disturb their work. The resultant feeling is one of annoyance, impatience, frustration towards alerts, prompts and other required actions (Krieger, 2009; Herzog & Shahmehri, 2007);
3. Users do not understand security messages and features. The lack of understanding compromises their information and the computer systems (Sasse, 2003; Herley , 2009; Krieger, 2009);
4. Users are not comfortable with making security decisions. (Sieger, Kirschnick, & Möller, 2011).
5. Users reject security advice (Herley, 2009).

These features invoke negative feelings in the users such as annoyance, impatience and frustration towards the feature. More on this was presented in Section 3.3.1 presented when interaction design is discussed.

In this regard, USec can also be defined as "*A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users*" (Herzog & Shahmehri, 2007). Issues related to usability and security are considered complex as they are independently regarded and both leave the user on the periphery. To deal successfully with USec the user should be at the centre and should influence the design of usable security. The security-usability threat model by Kainda, Flechais, and Roscoe, (2010) shows the most important aspects that should be considered when evaluating usability and security. The aspects are connected to usability or security or both from a novice user's perspective. Figure 3-4 is the threat model. Worth noting is the fact that knowledge and skill are the heart of user characteristics.

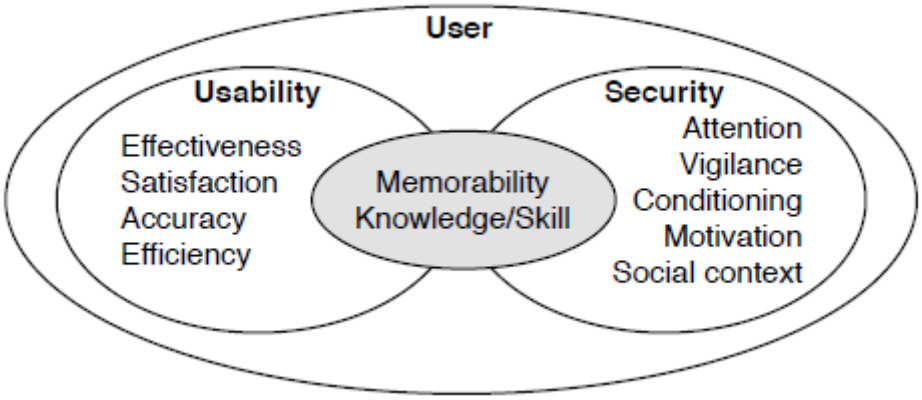


Figure 3-4: Security - usability threat model by Kainda et al. (2010)

To ensure that designed security is usable, users must be knowledgeable and skilled to use the security. There is a need to measure the extent of security usability problems in end user programs. Section 3.4.2.3 presents criteria that can be used to evaluate security usability.

3.4.2.3 Criteria for evaluating usability

Usability is the degree to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified environment of use (ISO 9241-11, 1998). This definition emphasises measurable attributes of a usable product, and these can be used as criteria to evaluate the extent to which the product is usable. The ISO9241 – 11 framework provides a basis for evaluating usability by showing the relationships among the different user-product interaction components. Emerging from extensive literature studies, Figure 3-5 presents a modification of the usability framework for this study. Components key to usable security, goals and criteria are presented.

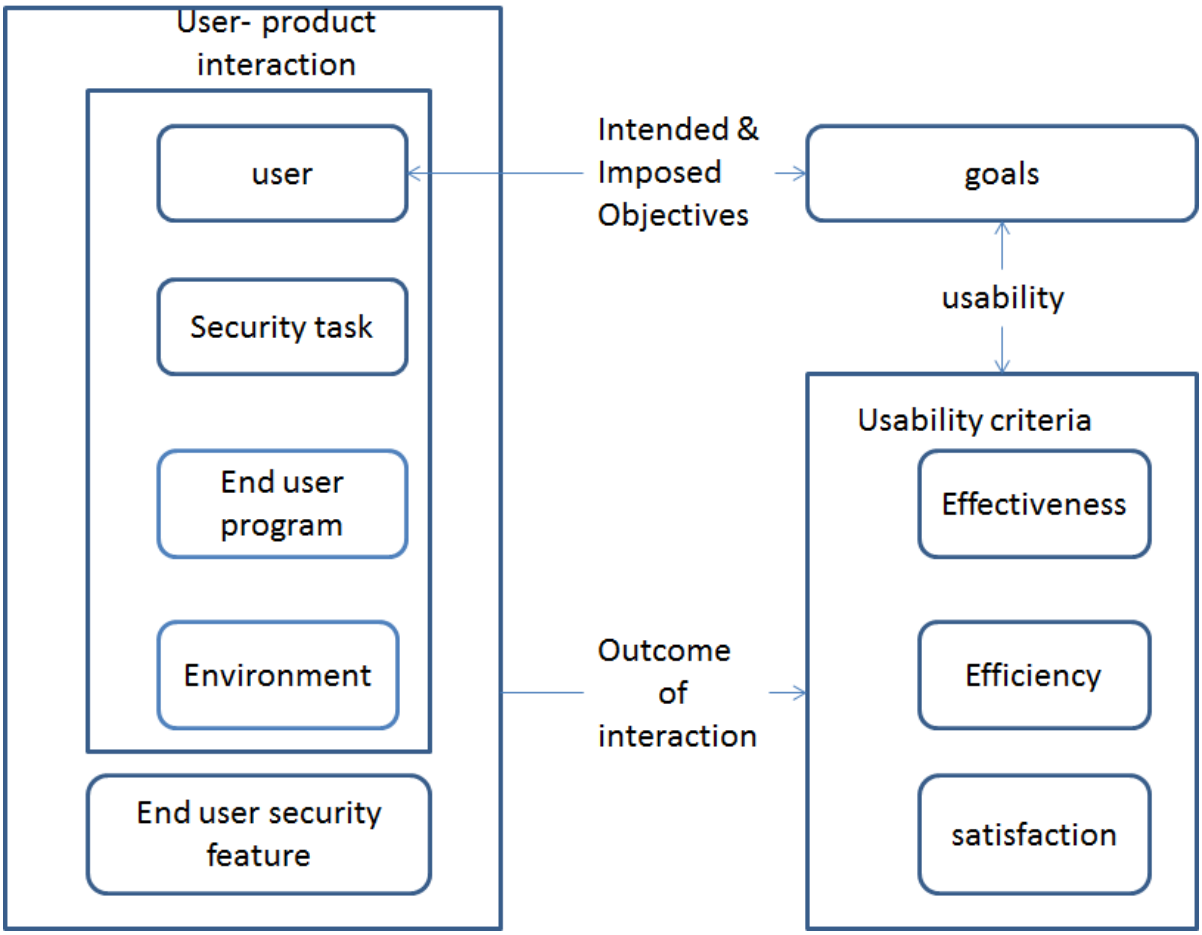


Figure 3-5: Modified usability framework by ISO9241 -210.2010

The product in this case is the security feature; the context of use is the end user program; the user's intended task is the security task in a work or leisure environment using devices that support the program and the user (with variable competence, awareness, and expectation). Security features interact with the user in an environment to perform a task using some device and this defines the user- product context of interaction. The outcome is a measure of effectiveness, efficiency and satisfaction with the interaction. **Effectiveness** is how well the users can achieve their goals (intended and imposed) and how usable the product is. **Efficiency** measures how much time and effort the user invests in the task to achieve their "goal" (security is not necessarily their goal in a EUP) as well as to what extent the product is usable. **Satisfaction** is the measure of how much the user enjoys using the product. Enjoyment is a characteristic of User experience with the product.

According to ISO/IEC 9126 (2001), usability is "A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users". The attributes include learnability, understandability, operability, efficiency,

effectiveness, ease of use and user satisfaction (Faulkener, 2000; Nielsen, 2000). Do the end user programs have security designs satisfying these required attributes?

The attributes can be used as the criteria to measure how usable a product is. Therefore **learnability, understandability, operability** and **ease of use** can be added to the list.

The criteria for evaluating usability include models of usability and usability heuristics. Heuristics are the principles used to evaluate the compliance of security features to usability principles. Nielsen's usability principles can be applied. These are **trust, ease of use, terminology, ease of learning, feedback, errors, help and documentation**. Similarly, criteria were presented by Yeratziotis et al., (2011) to evaluate two online heath systems.

In total, 13 criteria have been identified as **effectiveness, efficiency, satisfaction**, **learnability, understandability, operability**, **ease of use, terminology, feedback, errors, help and documentation.** To apply the criteria successfully there should be methods in place that can be followed. Section 3.4.2.4 focuses on usability evaluation methods.

3.4.2.4 Usability evaluation methods

There are three classifications of usability evaluation methods, namely testing, inspection and inquiry (Campbell, 2000).

Usability Testing (UT) involves selecting a sample of users to work on some representative tasks to demonstrate the extent to which the user interface enables users to perform their tasks. The following testing methods are used for UT: coaching methods, co-discovery learning, performance measurement, question-asking protocol, remote testing, retrospective testing, shadowing method, teaching method, and thinking aloud protocol.

Usability Inquiry (UI) involves gathering information about the end users' understanding, needs, likes and dislikes of the system through observations, conversations or interviews. Inquiry methods include: field observation, focus groups, interviews, questionnaires, logging actual use and proactive field study. In this study interviews were used for pilot studies and questionnaires for user studies. Field user studies allow for users to be evaluated in real time environments, on the other hand field studies can capture information on user behaviour, need analysis, heuristic evaluation and user satisfaction (Sharma, 2013).

Table 3-1 summarises the methods, providing information about when the UI method is applicable, at what stage of the product lifecycle, who is involved, where they should be located and the usability issue being tested. Stages are design, code, test and deployment with usability issues stated as effectiveness (E1), efficiency (E2) and satisfaction (S). The design stage has limited activity; therefore it is not included in the table.

Table 3-1: Typical usability inquiry methods

Inquiry	**Stage applied**			**Personnel needs**			**Remote**	**Usability issue**		
	code	test	Deployment	Usability experts	Software developers	users		E1	E2	S
Field observation	N	Y	Y	1	0	2	N	Y	-	Y
Focus group	N	Y	Y	1	0	6	N	Y	-	Y
Interviews	Y	Y	Y	1	0	2	N	Y	-	Y
Logging actual use	N	Y	Y	1	0	6	Y	Y	Y	-
Proactive field study	N	N	N	1	0	2	N	-	-	-

Interviews are also used at design stages. Proactive field studies can be used at requirements gathering as well as at design stages and with input from usability experts and users. Software developers have no role at this level. The tests are done with usability experts and end users only.

Several questionnaires are used for usability testing. Standardised questionnaires are categorised according to whether they are post-study, post-task, web or other (Sauro & Lewis, 2012). Table 3-2 lists some of the standard questionnaires (Sauro & Lewis, 2012):

Table 3-2: Standardised questionnaires

Acronym	Instrument	Reference
QUIS	Questionnaire for User Interface Satisfaction	Chin, Diehl, and Kent, 1998
SUMI	Software Usability Measurement Inventory	Kirakowski and Corbett, 1993; McSweeney, 1992
PSSUQ	Post-Study System Usability Questionnaire	Lewis, 1990a, 1992
SUS	Software Usability Scale	Brooke, 1996
PUEU	Perceived Usefulness and Ease of Use	Davis, 1989
NAU	Nielsen's Attributes of Usability	Nielsen, 1993
NHE	Nielsen's Heuristic Evaluation	Nielsen, 1993
CSUQ	Computer System Usability Questionnaire	Lewis, 1995
ASQ	After Scenario Questionnaire	Lewis, 1995
PHUE	Practical Heuristics for Usability Evaluation	Perlman, 1997
PUTQ	Purdue Usability Testing Questionnaire	Lin, Choong, & Salvendy, 1997
USE	USE Questionnaire	Lund, 2008

Of the presented questionnaires, QUIS, SUMI, PSSUQ, SU, ASQ and USE are post-study usability testing tools.

Usability Inspection involves usability experts or software developers, users and other professionals reviewing usability-associated features of a user interface. Inspection methods include: Cognitive Walkthroughs, Feature Inspection, Heuristic Evaluation, Pluralistic Walkthrough, Standards Inspection, Consistency Inspection and Perspective-based Inspection. Table 3-3 summarises the usability inspection methods, providing information about the stage of the product lifecycle where it is applicable; who is involved; where they should be located and the usability issue being tested. Stages are design, code, test and deployment with usability issues stated as effectiveness (E1), efficiency (E2) and satisfaction (S). The design stage has limited activity; therefore it is not included in the table.

Table 3-3: Typical usability inspection methods

Inspection Method	**Stage applied**			**Personnel needs**			**Remote**	**Usability issue**		
	Code	Test	Deployment	Usability experts	Software developers	Users		E1	E2	S
Cognitive Walkthroughs	Y	Y	Y	1-4	0-2	0	N	Y	-	-
Feature Inspection	Y	Y	Y	1	0	0	Y	Y	-	-
Heuristic Evaluation	Y	Y	Y	4	0	0	Y	Y	Y	-
Pluralistic Walkthrough	N	N	Y	1	1	2	N	Y	-	Y
Perspective-based Inspection										

Perspective based inspection, as applied by Zhang, Basili, and Shneiderman (1998) allows for usability inspection from a specific perspective at a time. Nielsen (1995) has three more inspection methods, namely standards inspection, consistency inspection and formal usability inspection. Usability is inspected from the perspective of the novice, expert and error handling use,using task scenarios.

3.4.2.5 Usability Heuristics are used to evaluate an interface or product for conformance to usability guidelines and whether or not a user can use it. Nielsen (1994) has developed ten usability heuristics for interface design. These are:

1. **Visibility of system status**

The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.

2. **Match between system and the real world**

The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. It should follow real-world conventions, making information appear in a natural and logical order.

3. **User control and freedom**

Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. This supports undo and redo.

4. **Consistency and standards**

Users should not have to wonder whether different words, situations, or actions mean the same thing. This follows platform conventions.

5. **Error prevention**

Even better than good error messages is a careful design that prevents a problem from occurring in the first place. It both eliminates error-prone conditions or checks for them and presents users with a confirmation option before they commit to the action.

6. **Recognition rather than recall**

Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.

7. **Flexibility and efficiency of use**

Accelerators unseen by the novice user may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. It allows users to tailor frequent actions.

8. **Aesthetic and minimalist design**

Dialogues should not contain information that is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.

9. **Help users recognize, diagnose, and recover from errors**

Error messages should be expressed in plain language (no codes), indicating the problem precisely, and suggesting a solution constructively.

10. **Help and documentation**

Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large. The next section discusses the user experience resulting from the interaction with systems designed for secure HCI.

3.5 USER EXPERIENCE

The field of UX has evolved over time. Figure 3-6 shows how the literature has evolved since 2000 and the main authors. Trends from 2010 to date focus on UX models and frameworks for UX design in general, and much has been done in Web applications; however, the same cannot be said about security and, in particular, about EUPSF.

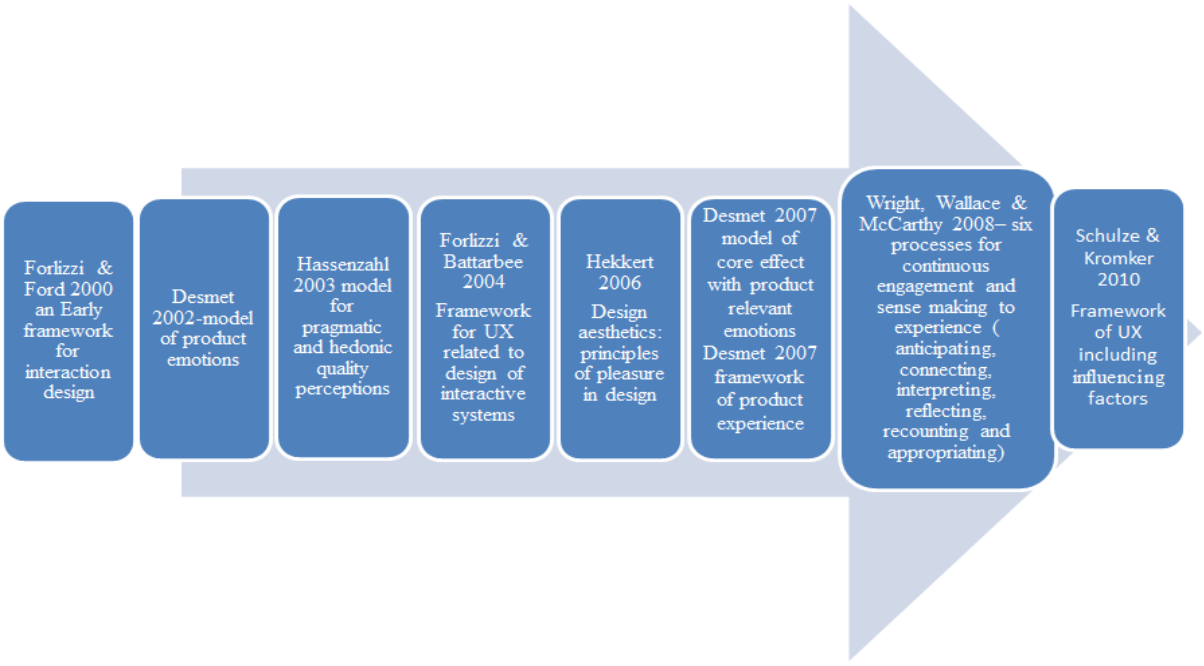


Figure 3-6: UX research progress (http://www.slideshare.net/NorthernUX/evaluating-user-experience)

User experience (UX) is an individual's perceptions and responses as a result (consequence) of the use or anticipated use of a product, system or service (ISO 9241-210, 2010). According to Garrett (2009), it is a combination of perception, action, cognition, and emotion. The UX dimensions are classified as external engagement (Perception: engaging the senses; and Action: engaging the body) and internal engagement (Cognition: engaging the mind; and Emotion: engaging the heart.) Wright , Wallace and McCarthy (2008) bring in another

dimension to experience called continous engagement and sense making. This dimension can be viewed as a combination of six processes, namely: anticipating, connecticng, interpreting, reflecting, recounting and appropriating (Wright, et al, 2008). Wright et al. (2008) argue that experience is created by uninterrupted engagement with the world through actions of sense-making at many levels, which can be captured in six processes. Anticipating is expecting an experience; connecting is relating to the situation or context of interaction; interpreting is when the user is describing the experience; reflecting (also referred to as immediate reflecting) is when the end user judges the experience; recounting goes beyond the reflecting to reflect it from the perspective of other users' experiences; appropriating relates an experience to past and future experiences.

The different definitions and comprehension of UX makes it even complex for novices in the field to understand and deal with it (Roto, 2007). To contextualise this research, the following user experience definition by Hassenzahl and Tractinsky (2006) is adopted:

> "a consequence of a user's internal state (predispositions, expectations, needs, motivation, mood, etc.), the characteristics of the designed system (e.g. complexity, purpose, usability, functionality, etc.) and the context (or the environment) within which the interaction occurs (e.g. organisational/social setting, meaningfulness of the activity, voluntariness of use, etc.)".

Figure 3-7 shows UX as a product of the user's internal state (values), and the characteristics of the designed system (product) in an organisational setup (context shaped by organisational values). It depicts the relationship between user experience, usability and human computer interaction in context. The context, in this case, is the organisation. The user has personal values which are inherent elements of their character and the organisation has values that are enforced through a number of policies and that reflect on their mission and vision. The UX is the outcome of the user's interaction with the product in a specific organisation. Product refers to the user perspective definition of UX, which focuses on emotional and aesthetic experiences as well as the experience of meaning during the user-product interaction.

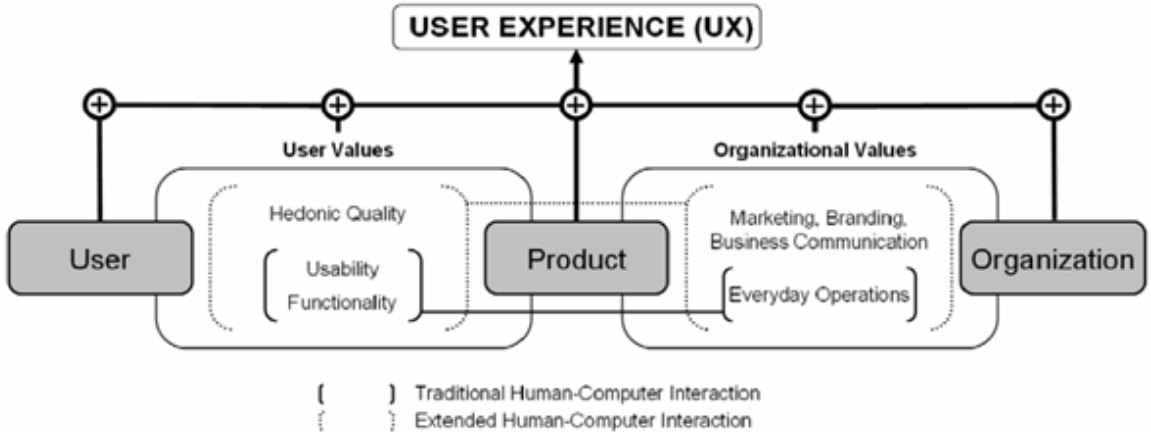


Figure 3-7: Simplified model of User Experience (Jetter & Gerken, 2007, p. 107)

User experience facets model UX as an intersection of three elements emotion and affect; the instrumental and the experiential aspects. Therefore UX can only exist in the presence of elements of the three perspectives. The user has variable moods that are the result of many environmental factors. Depending on their duties and on the reason for using the application program, they have a motive and expectations. The environment can be at work or at home and the purpose can be business, social or miscellaneous. As such, the environment has characteristics that influence how the user interacts with product and the tone in which they do it. These and prior experience or influence, as well as values and culture determine how users interact with a product. In the use of end user programs the motive is to complete a task that has nothing to do with security; therefore, there is no expectation of security interaction. However, as there are embedded security features in the EUPs, when the need arises for them to be activated, dialogues that require interaction will be presented to the end users for their action. The dialogues have their own characteristics that can deter or encourage the user to respond to them. Users can interact with their application security features while working, socialising or doing personal business, thus defining the context of interaction.

The overall UX of end user-security feature interaction is influenced by the user's cognition, by technical aspects of the EUP and by where or when the interaction occurs (Forlizzi & Ford, 2000). This presents a complexity to the designers as they have no way of controlling the human aspect, in particular. Product properties include quality, pragmatics and hedonics; these can be classified as instrumental (utility and usability) or non-instrumental (aesthetic, symbolic or motivational aspects). Owing to the complex nature of UX, different approaches and definitions are presented by authors and they vary according to perspectives.

Therefore, it is difficult to have the right assessment of UX by focusing on just one aspect as the overall UX is affected by all three. End users' perceptions of product quality is based on their experience of interaction and of the product qualities giving rise to effective use and pleasure (Sutcliffe, 2009).

Components of user experience (context, product properties and user attributes) presented by Minge (2008), determine interaction characteristics. The characteristics are emotional reactions, as well as instrumental and non-instrumental qualities, which create a perception of the product. Perceptions are mainly influenced by user awareness as it determines choice, the choice gives the first impression, and this impression determines the usage. If the experience is good, then the user can use the product all the time and the experience improves product awareness. However, the first impression can result in problems with product usage. This will give a bad experience and registers a negative impression of the product. The relationship of awareness, choices, impression usage, related problems and UX are shown in Figure 3-8.

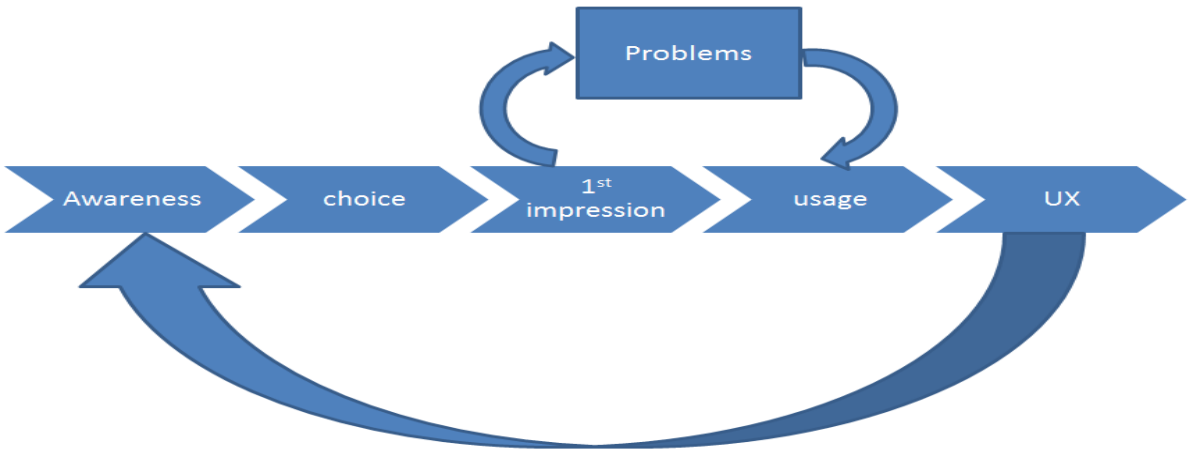


Figure 3-8: Awareness UX model

3.5.1 UX models and frameworks

UX models that are classified as structural establish relations (cause-and-effect) among concepts and enlighten the design of a system and measurement models to facilitate measurement of concepts in order to guide the assessment of a system (Law & van Schaik, 2010). Honeycomb, by Morville (2004,) and the modified one by Yeratziotis, van Greunen, & Pottas, (2011) are basic UX models that inform our research. The two models demonstrate the need to address security. The next section presents models and theories of experience.

3.5.2 UX Design

UX design is multidisciplinary as it cuts across HCI, industrial design, human factors and the ergonomics branches of sociology, physiology, cognitive science and philosophy; as well as architecture, computer science, and visual and sound design (Tariq, 2015). According to Garrett, (2009, p.1) "Experience design is the design of anything, independent of medium, or across media, with human experience as an explicit outcome, and human engagement as an explicit goal."

Human engagement is the goal of experience design, because the human is the most important part of any product design. Garrett (2009) defines engagement as a matter of a perception engaging the user's mind and all his senses (sight, sound, touch, smell, and taste) and classifies it as external or internal to the end user.

User experience design (UXD) focuses on the emotional aspects (internal engagement) of human experience such as happiness, although it is closely related to User-Centred Design (UCD) methods, which target human performance enhancement (Cummings, 2008). This approach is comparable to the holistic approach proposed by Wright et al., (2008). The holistic approach focuses on the sensual, emotional, and compositional, as well as the spatio-temporal aspects (Wright, et al., 2008). Since user experience comprises the overall end-users' perceptions (effectiveness, efficiency, emotional satisfaction, and quality of relationship with service entity) as they interact with a product or service (Kuniavsky, 2010), it is important that the design of EUP security features focus on embracing all these factors.

End users' perceptions of product quality are based on their experience of interaction (external engagement), and the product qualities giving rise to effective use and pleasure (Sutcliffe, 2010). What UX evaluation methods exist? Section 3.5.3 presents some of the evaluation methods relevant to this research.

3.5.3 UX Evaluation

User experience evaluation can be summative (end product) and formative (design and development). To evaluate the effect of a program's security features on UX, various criteria that influence the overall UX can be used. Some important aspects are security policies, usability (convenience, efficiency, understandable, visibility) (Furnell et al., 2005), user knowledge of security threats and solution/ mitigation strategies related to their application programs.

User experience (UX) evaluation means investigating how a person feels about using a system (product, service, non-commercial item, or a combination of them). It is complex to evaluate user experience and to come up with solid results, since user experience is subjective, context-dependent and dynamic over time (Law, Roto, Hassenzahl, Vermeeren, & Kort, 2009)

Laboratory experiments may work well for studying a specific aspect of user experience, but holistic user experience is optimally studied over a longer period of time with real users in a natural environment.

According to (Schulze & Krömker, 2010) UX is the degree of positive or negative emotions that influence future usage as a result of interaction in a particular context. This can be during or after interaction. Based on these and other UX definitions, three factors of interaction are identified as human (end user), product and the environment. HCI interaction is influenced by security feature properties, and user characteristics, as well as by contextual properties (Mahlke, 2008). Each of these factors can further be specified in context depending on the goals of the user and the product. The human factor has needs, perceptions, motives, goals, emotions, and competencies (Desmet & Hekkert, 2007). Product qualities are appeal, complexity, usefulness, efficiency, effectiveness, and behaviour sources, (Desmet & Hekkert, 2007). UX goes through a cycle with three stages: expectation/anticipation (before use), momentary during use and reflection after use (Schulze & Krömker, 2010). Yet the process of making sense of the experience can be considered as six different stages, as proposed by Wright , Wallace , & McCarthy, (2008): anticipating, connecting, interpreting, reflection, recounting and appropriating. Similarly, the senses can be viewed from the three stage cycle depending on when they occur in the stages of interaction.

Measurement of UX can be during a session (observation, physiology, experiments), or after a session (questionnaires) (Sutcliffe & Hart, 2011).

UX evaluation methods can be classified into five categories: all UX, method type, development phase, studied period of experience and evaluator / information provider (Roto, et al., 2012). Focus on the period of experience is important and that can be instant, occasional or complete UX (Roto, Vermeeren, Law, & Hoonhout, 2011). Periods can be classified relative to usage, as before usage (anticipated UX), snapshots during interaction (momentary/emotional), an experience/after use (of a task or activity- episodic) or long-term UX (cumulative) (Law E. L.-C., 2011; Roto et al., 2011) . The snapshots closely relate to the

UXEL framework, which presents UX from designer, user and enviroment perspectives of the product. The snapshots of UX defined as designer, which equate to before usage experience; and actual experience, which can be momentary, episodic or overtime, are used to connect user, designer and the enviroment. Figure 3-9 shows how users transit from one type of experience (snapshot) to another.

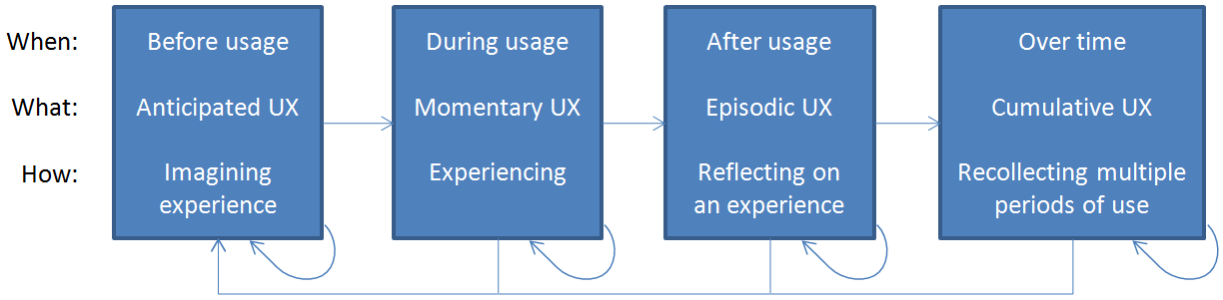


Figure 3-9: Snapshots during interaction (Roto et al., 2011)

Furthermore, evaluation methods can be classified according to type of evaluation context and type of data collected. Based on the CHI 2009 SIG classification, a choice was made to focus on approaches which consider evaluating UX jointly with usability, and user questionnaires for post-activity assessments, as well as expert evaluation using a heuristic matrix.

3.6 UX CRITERIA FOR EUP SECURITY FEATURES (EUPSF)

UX evaluation can be summative (end product) and formative (design and development) (Bevan, 2008). Since security features in end user programs are an end product, summative methods are the natural choice. To evaluate the effect of a program's security feature on UX, various criteria that influence the overall UX can be used. Some important aspects are security policies, usability (convenience, efficiency, understandable, visibility) (Furnell et al., 2005), user knowledge of security threats and solution/ mitigation strategies related to their application programs. Colabro (2012) states that end user behaviour is directly linked to emotional satisfaction; hence, it is an important aspect to evaluate. To answer the posed question: "Which UX metrics/evaluation criteria can be used to determine the UX of end user program security features?", proposed criteria are presented as in Table 3-4. The listed criteria is a result of extensive literature studies on UX metrics for security in general

Table 3-4: Proposed criteria

Criteria	Author
Awareness/expected	Herzog & Shahmehri, 2007; Krieger, 2009
Motivating	Hassenzahl, 2004; Hassenzahl & Tractinsky, 2006; Herzog & Shahmehri, 2007; Cranor, 2009; Krieger, 2009; Sieger, et al., 2011; Lew, et al., 2010; Preece, 2002, 2002; Desmet & Hekkert, 2007; Schulze & Krömker, 2010
Comfortable	Herzog & Shahmehri, 2007; Krieger, 2009; Moller, 2009; Cranor, 2009; Sieger, Kirschnick, & Möller, 2011; Whitten and Tygar (2003)
Useful	Morville , 2004; Yeratziotis, 2011; Desmet & Hekkert, 2007
Desirable	Morville , 2004; Yeratziotis, 2011
Accessible	Morville , 2004; Yeratziotis, 2011; Rubin & Chisnell , 2008; Lew, et al., 2010
Visible / readily displayed/ findable	Nielsen, 1994; Yee, 2002; Johnston, Eloff et al., 2003)Furnell et al., 2005; Morville , 2004; Katsabas et al., 2005Yeratziotis, 2011; Cranor, 2009; Herzog & Shahmehri, 2007; Krieger, 2009
Valuable/ impact of use	Morville , 2004; Yeratziotis, 2011
Usable	Morville , 2004; Lew, et al., 2010; Yeratziotis, 2011
Supported	Shahmehri, 2007; Cranor, 2009; Krieger, 2009;
Understandable/complexity/ learnable	Shahmehri, 2007; Cranor, 2009; Krieger, 2009; Rubin & Chisnell , 2008; ISO 9241-210, 2010; Lew, et al., 2010; Desmet & Hekkert, 2007
Long term experience/ memorability	Moller et al., 2009, Nielsen, 1993; (Ravdev & Johnson, 1989)
Security/ safety	Lew, et al., 2010; Yeratziotis, 2011; Lew, et al., 2010; Preece, 2002
Efficient	Nielsen, 1994; Faulkner, 2000; Furnell et al., 2005; Desmet & Hekkert, 2007; Kuniavsky, 2010; Rubin & Chisnell , 2008; ISO 9241-210, 2010; Lew, et al., 2010; Yeratziotis, 2011; Sharma, 2013
Effective	Nielsen, 1994; Faulkner, 2000; Desmet & Hekkert, 2007; Kuniavsky, 2010; Rubin & Chisnell, 2008; ISO 9241-210, 2010; Lew, et al., 2010; Yeratziotis, 2011; Sharma, 2013
Satisfaction	Nilsen, 1994; Lew, et al., 2010; Rubin & Chisnell , 2008; Preece, 2002; (ISO 9241-11, 1998)
Exciting/perception/ emotion	Herley, 2009; Desmet & Hekkert, 2007

3.7 SUMMARY

This chapter presented human computer interaction, interaction design, user-centred design, human computer interaction security, usability, usable security and user experience. Technology is designed for people; however, people can use it effectively if the field of HCI has design principles that ensure that the technology is usable. Interaction design principles produce user-centred products. Usability of products influences user experience and behaviour. Security can be designed to be usable by applying usability and HCISec principles.

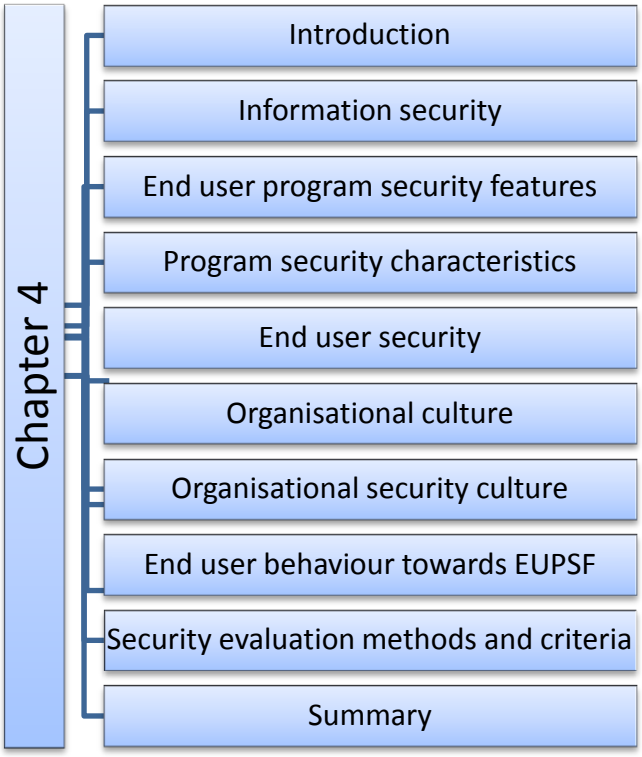
User experience is a measure of emotions, enjoyment and other feeling associated with an interaction. In summary, a lack of tools to evaluate UX exists coupled with a lack of metrics for application security features to measure awareness levels of case subjects. In the next chapter literature on InfoSec is presented.

CHAPTER 4: INFORMATION SECURITY FEATURES

4.1 INTRODUCTION

What are the suitable security criteria/ methods that can be used to evaluate UX of end user program security features?

This chapter focuses on the end user program security. The field falls within two disciplines, namely Information security and User experience (UX), a subsection of Human and Computer Interaction (HCI). Firstly, information security is presented; thereafter, the concepts of usable security can be comprehended, end user programs' security features, security awareness, security metrics, security evaluation methods and finally, the summary will be presented. The goal is to establish literature on security usability, and how end user program security fares. The outline in the chapter map will be followed.



4.2 INFORMATION SECURITY

Information in computers is processed data that is stored or transmitted on computer systems. Information security (InfoSec) is a process that includes protecting information integrity, confidentiality and availability on computers and shared over networks (Ciampa, 2011). InfoSec has the following goals: confidentiality, availability, authenticity, nonrepudiation, integrity, privacy, authenticity and trustworthiness, reliability, auditability and accountability on devices that store, manipulate and transmit the information through people, products and procedures (Cherdantseva & Hilton, 2013; Ciampa, 2011; Pfleeger & Pfleeger, 2007; Stalling & Brown, 2008; Whitman & Mattord, 2011).

USec aims to improve the usability of security features in end user programs, focusing on the design, evaluation and implementation of interactive secure systems. Good security for an organization has multi-layers in place to achieve all the security goals (Whitman & Mattord, 2011; Ciampa, 2011). The layers are physical, personal, operations, communication, network and information security. An information security breach comprises a threat, carried out by an attacker who exploits/takes advantage of security loopholes/weaknesses or vulnerabilities to gain entry (Pfleeger & Pfleeger, 2007). Lately there has been advancement in attack mechanisms

used by cyber criminals in their attempts to breach information security. Top of the list is social engineering, especially phishing attacks. Both of these attacks target the human factor of security that has been cited as the reason for breaches (Whitten & Tygar, 2003). Security can also be viewed from a business perspective. The business model of information security comprises people, technology, process and organisational aspects. They interact to ensure the objectives of security (von Roessing, 2010). The different aspects are linked by dynamic indicators, namely human factors, culture, architecture, governing, and emergence, as well as through enabling and support, as shown in Figure 4-1.

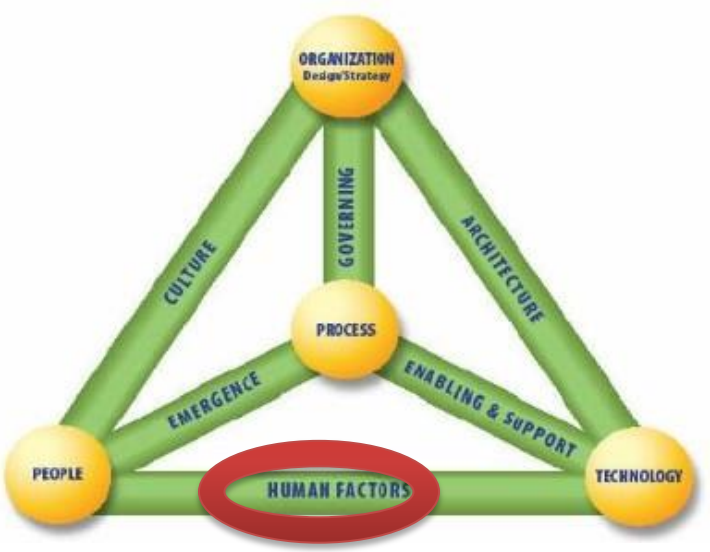


Figure 4-1 Business model for information security (BMIS) (ISACA, 2009)

The research focuses on human factors as dynamic interconnectors between people and technology (highlighted in red) and would like to propose a process that influences security culture, emergency and provide enabling support. To do so, there is a need firstly to understand the security challenges for humans.

A threat is defined as a potential violation or breach of security. Examples of threats are unauthorized disclosure of information that violates the confidentiality goal of security, deception, disruption and usurpation (Stalling & Brown, 2008, p. 15). These can also be classified as interception, interruption, modification and fabrication (Pfleeger & Pfleeger, 2007, p. 7). When a threat is carried out successfully, it is an attack or security breach.

In recent times it has become difficult to defend against attacks because:

1. The number of devices on the Internet has increased tremendously (Ciampa, 2011; Statistics, Internet World, 2011);
2. The speed of attacks is high; there has been an advancement of attack mechanisms (Whitman & Mattord, 2011);
3. The attack tools are easy to access and not complex to use (Whitman & Mattord, 2011);
4. The attack tools are as available to black hackers as they are to security professionals (Long, 2012);
5. The detection of vulnerabilities is faster by black hackers compared to white hackers (Long, 2012).

The increase in attacks is also attributed to delays or the absence of patching, updating and upgrading of application software (Shackleford, 2011). As a result of this attackers are now using social engineering to gain entry into systems by manipulating vulnerable programs running on client side machines which, for the purpose of this research, will be defined as end user application programs (EUP) (Ciampa, 2011). Information security is designed for users to secure their electronic information. The next section discusses user security.

4.3 END USER PROGRAM SECURITY FEATURES

Information Security is focused on procedures, people, devices and communication of information in an integral and confidential way (Whitman & Mattord, 2011). To protect the end user's information, end user program developers have embedded security features in the applications (Furnell, 2005). The security features are designed to protect individual and organisation security from cyber criminals. They offer end user program assurance, which is defined as "the application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner; are free from accidental or intentional vulnerabilities; provide security capabilities appropriate to the threat environment; and recover from intrusions and failures" (Mead et al., 2010).

In practice, every designed program has threats, vulnerabilities and attacks specific to its operational domain and, as such, security features are designed to assure security within the program context. Some of these features interact with users to protect their information while others run in the background (Furnell et al., 2005). Interaction can be updating the application,

deciding on a security action or even configuration. In most cases the security features seldom prompt the users for their input; because of this, the user does not know how to handle the rare occurrences appropriately. As a result of improper interaction, users present themselves as easy targets for cyber-attacks (SANS, 2011; Whitman & Mattord, 2011).

Security features include alerts, dialogue boxes, security agents, office assistant, update features, permissions and encryption, among others. These features are designed to be suitable and effective for the programs; however, security of the systems depends on the users using the security (Furnell, 2004).

4.4 PROGRAM SECURITY CHARACTERISTICS

Program security has characteristics that influence the behaviour of users towards the execution/implementation thereof. According to Herzog and Shahmehri (2007); and Whitten and Tygar (2005), the features include that:

1. Security is not the primary responsibility for the user; hence, they do not have the commitment to learn and understand it.
2. Security is regarded as a bother/abstraction from the primary task as they are usually required to respond or interact with a number of dialogue boxes to complete a single security task.
3. Security features (alerts, dialogue boxes) are rarely displayed.
4. It is complex for users to understand and implement.
5. Sometimes options presented to the users do not lead them to making the right security choice for the user.

Research in the area of HCISec has established that the mentioned features make application security unusable, as in the following examples: Firewall by Johnston et al (2003), Wool (2004); Zone by Katsabas et al. (2005); Internet Explorer by Furnell (2006); Mozilla Firefox by Katsabas, et al. (2005); Microsoft Word by Furnell (2005); and Katsabas et al. (2005), Outlook Express by Furnell (2006); encrypting email by Whitten & Tygar (1999); Login systems by Sasse (2003) and several others. Software developers have designed necessary and effective security in their programs. For the security to be effected it depends on the user to use it appropriately (Furnell, 2004). Embedded security design does not answer user questions, but

instead follows in-built rules that were determined by the program designers. The user questions, according to Baecker et al., (1995 p.670) cited in Herzog and Shahmehri (2007) are:

1. Informational: What can I achieve with this application?
2. Descriptive: What is this? What can it do?
3. Procedural: How do I do this?
4. Interpretive: What is happening? Why? What does it mean?
5. Choice: What can I do?
6. Guidance: What should I do?
7. History: What have I done?
8. Motivational: Why use the feature? What is the benefit?
9. Investigative: What else should be known?

Question 8 is very important, specifically when considering security as a secondary task for the user (Herzog & Shahmehri, 2007). Research has shown that users are strongly motivated to protect their information and are aware of security threats. However, they do not understand the security features to implement them correctly. Furnell (2006) gave the reasons as: the use of technical jargon, unclear functionality, the lack of feedback and forcing uninformed decisions (owing to lack of knowledge). One way of improving security is by answering the question, whilst an understanding of the typological setup of organisational culture can help achieve this. The next section addresses what an organisational security culture is and its components.

4.5 END USER SECURITY

User security deals with procedures and policies to ensure that a user can achieve personal security of their information. User-centred security speaks of "security models, mechanisms, systems and software that have usability as primary motivation or goal" (Zurko & Simon, 1996, p. 27).

A user is a person or device that uses a computer system to perform some task. The users can be classified as procedures that trigger some action on the machine, an expert/technical user who develops, maintains or administers the system and an end user who uses applications running on the machine to do their work. The human users have varying levels of knowledge and

appreciation of security features and programs running on their machines, and are vulnerable to different breaches. For example, developers are exposed to buffer overflows and other programming coding errors, while end users can experience phishing, viruses, inconsistent errors, etc.

User categories are also based on aspects related to (Beisse, 2004):

1. The environment: home or corporate.
2. Skill level: experts, scientists, novices, average, advanced, designers, cybernut, programmer, engineer, and administrator.
3. Location: internal, external, guest, or remote.
4. Application: word processing, accounting, databases, email, publishing, and so forth.
5. Frequency of use: frequent, occasional, and persistent.

User security can thus be defined as technologies, mechanisms and processes that protect the end user, regardless of their category. End users mainly encounter security at three levels while they interact with computers. The first one is the operating system related security, for instance, they might be required to boot up with a password; logon with a password to the local machine or to the domain. Once they have logged on the computer, they can encounter security systems running on the system. The security system can be a firewall, intrusion detection/ prevention system, or the most common one - an antivirus. The first two security systems usually run in the background popping up alerts only when user intervention is necessary; however, because many attacks at this level involve malicious codes, more prompts from the antivirus and interaction are common. The end user uses application programs to accomplish their work-related tasks on a daily basis. This brings us to the frequent and third security that they encounter, program security features. End user program security features are part of the programs used to do work on a regular basis and to protect information processed by the program. The next section presents end user program security features.

4.6 ORGANISATIONAL SECURITY CULTURE

Organisational culture is “a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration that has worked well enough

to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." (Schein, 2004, p. 17). The behaviour of employees is influenced by the corporate culture eventually contributing to the organizational effectiveness (Thomson & von Solms, 2006). A corporate culture should, ideally, incorporate InfoSec controls into the daily practices and employee behaviour (Thomson & von Solms, 2006).

According to Schein (2004), there are three levels of culture: artefacts; espoused beliefs and values, as well as underlying assumptions. Artefacts consist of the visible and audible elements of culture that can be easily interpreted by employees, customers and the public (Schein, 2004).

Values and beliefs at conscious level that are based on prior learning support artefacts as they guide behaviour (Schein, 2004). These are mostly established by management in order to monitor and control how employees behave in the organisation. These can include ethics, code of conduct and communication.

Basic assumptions in reality represent and capture an organisation's culture as perceived by employees (Schein, 2004). These basic assumptions include the basic assumptions of members of a group or organisations as a result of shared learning experiences (Schein, 2004, p.22).

Culture is dynamic and is influenced by environmental, internal and external factors to the organisation as humans bring in their own individual cultures. There are seven dimensions to culture, as presented by Schein (2004). Since security is about interaction with technology, of interest is the nature of human activity and the nature of human nature that focuses on the character and appropriateness of human behaviour.

Interviews, questionnaires, or survey instruments can be used to study a culture's values, norms, ideologies, charters, and philosophies (Schein, 2004). Open-ended interviews can gather feelings and thoughts, but questionnaires and surveys limit the information collected as they specify bounds through the type of questions posed. A deeper study through intensive observation, concentrated questions, and user studies of purposefully selected motivated members of the group can reveal underlying assumptions that define perceptions, thoughts, feelings, and behaviour (Schein, 2004). These will enable a richer understanding of a phenomenon under study in context.

The BMIS positions culture as the dynamic interconnector between the people and the organisational security strategy as depicted in Figure 4-1(von Roessing, 2010). As the focus is on the organisation security strategy, it is important to understand its security culture. Models and frameworks of InfoSec culture have a basis in organisation culture literature, as presented by Detert, Schroeder, & Mauriel, (2000). However, different authors have different views on whether InfoSec culture should be incoporated in oganisational culture or should stand alone. The framework by Joo, Chang, Maynard, and Ahmad (2009) demonstrated that it is highly beneficial to incoporate InfoSec culture into organisational culture.

According to von Solms (2000), information security culture is part of the third wave of InfoSec: institutionalisation. The third wave is characterised by InfoSec standardisation, InfoSec Certification, cultivating an InfoSec culture and implementing metrics that always measure Infosec aspects (von Solms, 2000). As a culture, Infosec can be the natural way of operation by employees. This can infer that it is a component of orgnisational culture. Like culture, security culture is learned; therefore security learning models can aid organisations to create their own cultures.

Alfawaz, Nelson, and Mohannak (2010) developed a conceptual framework of InfoSec, which models how knowledge, skills and values influence InfoSec practices. They classified the practices into four modes which speak to different organisational cultures. Mode 1 is infancy, where nothing is in place, or technical requirements are in place, but not communicated to the end user, i.e. Von Solms's first wave is in place and may be a part of the second wave also. Mode 4 is the ideal situation and speaks to the third wave; culture has been intitutionalised. The four modes and their descriptions are shown in Table 4-1:

In this study there will be no enumeration of the level of organisational security, but will use the modes to identify the state of the institution under study. With this understanding it will be possible to position the InfoSec culture needs and their impact on user behaviour and experience with InfoSec features.

Table 4-1: InfoSec behaviour modes adopted from Alfawaz et al., 2010

Mode	Name	Description
1	Not Knowing- Not Doing	End users do not know the organisation's requirements for information security, such as policies in place and their requirements; they also are not educated on security. Consequently they do not behave correctly with regard to set security standards and best practices.
2	Not Knowing- Doing	End users do not know the organisation's requirements for information security, such as policies in place and their requirements; they also are not educated on security. However, they behave as expected.
3	Knowing- Not Doing	End users know the organisation's requirements for information security, such as policies in place and their requirements; they are also educated on security. However, they do not follow the requirements.
4	Knowing- Doing	End users know the organisation's requirements for information security, such as policies in place and their requirements; they are also skilled on security behaviour and they follow the requirements.

According to Chia, Ruighhaver, and Maynard (2002), investing in state of the art information security infrastructure and, at the same time, lacking a security culture to support end-user security, will be unprofitable for an organisation. Having looked at culture as one influencing factor, there is a need to consider technical aspects also. The next section presents end user behaviour towards security.

4.7 END USER BEHAVIOUR TOWARDS SECURITY

Furnell et al. (2005) carried out a survey to identify the challenges of understanding end users. They observed that the manner in which users are presented with security related decisions usually complicates the processes, resulting in them being unable to use the security aspects that they prefer or that are required of them. They targeted Microsoft Word, Outlook and Internet Explorer and their findings expose some complex areas, in which standard security features were poorly used by many of the sampled users (above average IT literate). Based on their findings they recommend better security functionality presentation to enable users to protect themselves. Recommendations include user training on: application security and how best they can use it,as well as security threats that they are exposed to when they connect to a network and how to manage them. They recommended further research in usability and security areas. To implement some of these recommendations there is a need to understand program security, since program

security has its own inherent complexity. This chapter set out to answer the question: "What are the suitable security criteria/ methods that can be used to evaluate UX of end user program security features?", the next section presents security product evaluation methods and criteria.

4.8 SECURITY PRODUCT EVALUATION METHODS AND CRITERIA

From a technical perspective, security product evaluation methods and criteria examine relevant security parts of a program or system for compliance with security frameworks and methodologies. Current evaluation standards outlined in literature include Information Technology Security Evaluation Criteria (ITSEC) used by the European Union (EU); Trusted Computing Security Evaluation Criteria (TCSEC) used by the United States (US); Common Criteria (CC) - Hybrid of ITSEC and TCSEC, is a framework useful as a guide for the development, evaluation and/or procurement of (collections of) products with IT security functionality. INFOSEC Evaluation methodology (IEM) is used to assess vulnerability in systems and to validate the actual INFOSEC posture of those systems. INFOSEC Assessment Methodology (IAM) is a standardized baseline for the analysis of the INFOSEC posture. However, this is not applicable to features incorporated in non-security programs (Saint-Germain, 2005). Security Product Evaluation Methods and Criteria examine security relevant parts of a program or system for compliance with security frameworks or methodologies.

Evaluation frameworks or methodologies and programs establish confidence in the security product vendor from the customer. They can assist security professionals in developing, implementing, and monitoring as well as in the maintenance of security programs (von Roessing, 2010). "Although there are no frameworks dedicated to information security at this time, there are many risk frameworks that may be of use" such as OCTAVE, COBIT, ITIL and ICIF (von Roessing, 2010). OCTAVE is a risk framework while ITIL is a management framework; on the other hand, COBIT and the international control integration framework have governance and the management of IT as their focus.

Usability metrics measure usability dimensions such as effectiveness, efficiency and satisfaction (Sharma, 2013). According to Sauro and Kindlund (2005), (as cited in Sharma, 2013), metrics for measuring usability are: task completion, error counts, task times, and satisfaction scores.

It is evident that there are no models, criteria and frameworks to evaluate EUPSF. In pursuit of our goal to come up with evaluation criteria for EUPSF, the next section focuses on security usage in general.

4.8.1 Security usage

The security features of any program that are configured and implemented by end users; the success significantly depends on the user's interaction with the information presented by the feature, the choices of program users, and the impact of their actions. According to Adams and Sasse (1999), inadequate security communication with end users during design results in security mechanisms that present overheads, or oblige unworkable user behaviour; hence, many users have a tendency to circumvent such mechanisms. Security mechanisms and policies that are not user-centric and do not focus on users' work performance, organizational strategies, and usability can result in security breaches and poor security (Adams & Sasse, 1999).

Yee (2002) established ten principles for designing security from a user-centred point of view focusing on user interaction design in secure systems. If security is designed with users in mind, then the interaction with the features should fulfil the usability metrics (principles). Table 4-2 presents Yee's ten design principles for secure system interaction

In this study, it is assumed that program security features meet these criteria. Heuristic evaluation will be used in Chapter 5 to investigate and validate the usability of the security features. Assuming that these principles hold true, the next section will discuss metrics for security evaluation.

Table 4-2: Design principles Yee, 2000

Number	Principle	Description
1.	Path of least resistance	The most accepted way to complete any task should also be the most secure way.
2.	Appropriate boundaries	The interface should uncover, and the system should apply, distinctions between objects and between actions along boundaries that matter to the user.
3.	Explicit authorisation	A user's privileges must only be made available to other actors as a result of an clear user action that is understood to imply permitting.
4.	Visibility	The interface should allow the user to review any active actors easily and to privilege relationships that would impact security-relevant decisions.
5.	Revocability	The interface should permit the user to withdraw privileges easily that the user has granted, wherever withdrawal is possible.
6.	Expected ability	The interface must not give the user the impression that it is possible to perform impossible actions.
7.	Trusted path	The interface must provide an unspoofable and faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf.
8.	Identifiability	The interface should enforce that distinct objects and distinct actions have unspoofably identifiable and distinguishable representations.
9.	Expressiveness	The interface should provide enough expressive power (a) to describe a safe security policy without undue difficulty; and (b) to allow users to express security policies in terms that fit their goals.
10.	Clarity	The effect of any security-relevant action must be clearly apparent to the user before the action is taken.

4.8.2 Security metrics

Metrics are the result of a process. They are conceptual data repositories used to define and to standardize information. Metrics do not organise information into knowledge; they record observations. People are responsible for knowledge generation (Hayden, 2010). Unlike metrics, a measurement is observing and collecting data to gain concrete understanding of the phenomena under investigation (SANS, 2012). Security metrics provide information about IT security including costs and risks (asset value, threat and vulnerability are elements of overall risk) and must be based on a rigorous approach for security measurement and applied understanding seeking information security (Hayden, 2010).

Worthwhile metrics reflect the degree to which security goals are being achieved and they motivate actions taken to advance the security program of an organization. They can also pinpoint the risk levels of not implementing certain actions and can be used to improve the levels

of awareness within the organization (Payne 2006). According to Hayden (2010), security occurs as a result of human activity. Dimensions of vulnerability include the level of understanding of security concerns by computer users.

Jelen (2001) in SANS (Payne, 2007) defined metrics as derivations of comparing two or more measurements taken over time, while a measurement is a single point of view of specific, discrete factors. Useful metrics reflect the degree to which security goals such as data confidentiality are being met and they drive actions taken to improve an organisation's overall security program. They can also identify the risk levels of not implementing certain measures and can be used to raise the levels of awareness within the organisation.

This study focuses more on measuring the third element of risk- vulnerability. Facets of vulnerability include the degree of understanding of security issues among computer users. Are there any best practices to follow in developing security metrics?

Below are three security metrics lessons that can be used in developing an effective security metrics program in an organisation, as presented by Hayden (2010):

1. **Security Metrics Lesson #1**

   Security metrics and consequent risk-management choices will improve as you develop your skill to collect, analyse, and understand data regarding security operations.

2. **Security Metrics Lesson #2**

   Security is a business process that needs to be measured and controlled.

3. **Security Metrics Lesson #3**

   Security is the result of human activity. Effective measurement programs make an effort to understand people as well as the technology they use.

Payne (2006) defined steps to develop a process for a security metrics program. These are:

1. Define the metrics program objectives and goals (provide metrics that communicate clearly how user experience with security interaction in end user programs can be improved through awareness to ensure that embedded security features are used effectively and efficiently for better user and organisational security. The goals are to

base the metrics program on improving awareness within our organisation; to communicate the metrics effectively to all stake-holders including end users).

2. Decide on which metrics to generate (identify a specific security process to adopt) such as a compliance-based approach where you evaluate whether established standards (which need to be identified first) are being followed. If there is no framework in place, use a top-down or bottom-up approach to determine which metrics can be desirable to use. Start with goals and measurements to generate the metrics). Table 4-3 illustrates the top-down approach.

Table 4-3: Top down approach

1. Define the objectives of the security features.	To increase the policy awareness in the organisation.	Example objective for this study
2. Identify the progress towards each objective.	Current ratio of policy awareness compared to baseline 2012 survey figure.	
3. Determine measurements for each metric.	Number of people trained on security policies in the organisation.	

In this case some measurements were already done therefore the bottom-up approach in Table 4-4 can be adopted:

Table 4-4: Bottom up approach

1. Identify measurements that can be collected for this process.	Percentage of people who are not aware of security policies in the organisation
2. Determine metrics that can be generated from the measurements.	Train and improve the number of people aware of security policies since the last survey period
3. Determine the association between derived metrics and established objectives of the overall security program.	To increase security policy awareness among end users

The security industry already uses several commonly recognized metrics today to measure aspects of organizational IT security including:

1. Risk matrices
2. Security vulnerability and incident statistics
3. Annual loss expectancy (ALE)
4. Return on investment (ROI)
5. Total cost of ownership (TCO)

These metrics can be limited severely in terms of the value they bring to a security program as the measures are usually not well understood, and there is a tendency to measure aspects of security that are different from what their users believe they are measuring, regardless of being widely accepted.

“The importance of quality data, the focus on security as a business process, and a greater respect for the role of people and social interactions in the security process are all important elements of a successful security metrics program” (Hayden, 2010).

Several metrics have been identified to measure the usability of products or user interfaces. These focus on the hedonics and the pragmatics of the products. A vital aspect to encourage product use is to educate the user with regard to the existence and the benefits of using it and, as such, there is a missing element.

4.9 SUMMARY

This chapter discussed InfoSec focusing mainly on usability, Usable Security (USec), organisational security culture, security usage and end user program security features. These areas define the study premise. Information security was defined and focus was placed on embedded features in programs whose primary function is not security. This set the context for user interaction with these features as they primarily use the program for other purposes that are not security specific. The main objective is to be able to evaluate the UX of interacting with end user program security features. The basis of this objective is the assumption that security features are user-centred; therefore, their design conforms to usability guidelines. To validate this assumption, usability evaluations will be carried out on selected end user programs. Of the presented three usability evaluation methods (usability testing, usability inquiry and usability inspection), questionnaires from the UI methods, as well as heuristic evaluations and cognitive

walkthroughs, will be used in Chapter 5 to carry out the usability tests. Usability frameworks, models and attributes were discussed and applied to the study parameters. The ISO9241-210 framework was applied to the study through literature review and a modified context-specific version is presented in Figure 3-5. Security usage in general was studied and general trends were noted; user behaviour is identified as a major concern. As the study focuses on the user perspective, literature on organisational security culture and a business model for information security was analysed. Worth noting was that awareness, knowledge, skills, values and basic assumptions play a crucial role in whether the user will or will not use embedded features. Navarro (2007) also states that "*with the right training, employees can become an organization's strongest security asset*". Awareness metrics design processes that are applicable to the study were also presented and metrics to measure awareness levels of case subjects were noted. The next chapter presents the data collection in a case study setup.

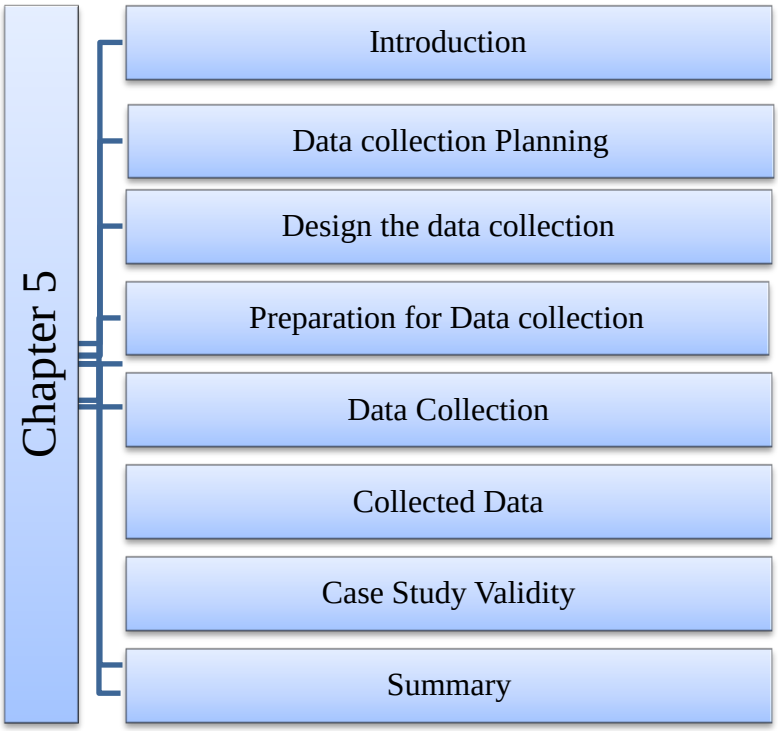
CHAPTER 5: DATA COLLECTION AND FINDINGS

5.1 INTRODUCTION

Based on observations by the researcher, as well as the results of the pilot study discussed in Chapter 1, the formal data collection process was informed. The empirical user study was conducted in a typical ICT enabled environment. This chapter presents the case study of an academic institution that uses information technology to support its processes. The case study addresses Research Question 1 and the objective is to come up with factors influencing UX. The question addressed by the study is:

What are the factors affecting UX with embedded security features in end user programs?

The chapter will follow the outline presented in the chapter map.



5.2 DATA COLLECTION PLANNING

Literature on HCI and InfoSec was presented in Chapters3 and 4 respectively. Based on the literature review, a theoretical framework was developed and is used to direct the study. To understand components of the framework in detail, it became imperative to conduct a case study of the phenomena. The purpose of the case study was to evaluate the importance of the theoretical framework components identified in literature studies by surveying end users in an organisation who use programs and their embedded security features to accomplish their daily tasks. A single case empirical study was conducted in a site where employees of the case organisation are identified as the end users and therefore termed participants.

5.2.1 Overview of the case study

The Polytechnic of Namibia is an academic institution in Namibia located in the nation's capital city, Windhoek. Namibia is one of the developing countries in Southern Africa which has become a hub of technology as it houses a landing point for the WACS. This brought about increased Internet connectivity, coupled with government efforts to ensure that everyone is computer literate. This presents a security challenge to InfoSec. The nation is still in the infancy of developing a computer emergency readiness team (CERT); hence, it is an interesting case to study. The institution has a student enrolment of 13400 per annum and employs 670 full-time staff. Of the 670; 350 are academic staff members and the rest are support staff. Each staff member has a desktop computer (PC) and/or laptop allocated to him/her upon employment. The student laboratories and library are equipped with PCs, which are used for practical sessions, as well as for information searches on the Internet and on e-library resources. Each PC has a Windows or Ubuntu operating system installed for daily business activities. Laboratories mainly use Windows, although in some departments Centos, Ubuntu, or MAC OS are used. Typical application software includes Microsoft Office, Internet browsers, integrated tertiary system (ITS), document readers (Acrobat), anti-virus software (Kaspersky lab), and email clients (mainly Thunderbird).

5.2.2 Sampling

Purposeful heterogeneous sampling was employed for selecting the case site as it allows for an in-depth study of one case to gain rich insights into the phenomenon (Saunders et al., 2009). The site has the typical elements in an IT driven organisation such as people, processes and

technology. The elements are dynamically connected by culture, human factors, governance, enablers, support, etc. The case is one of many similar cases worldwide; its study will provide a baseline for studying similar cases.

The participants in this research comprised lecturers, administrators and other professionals who make up the University community. The population was selected to show the diversity of users, who use similar programs for similar purposes to achieve different objectives from different backgrounds and professions. The participants were conveniently selected for the pilot study to give the views of both technical support and typical users, for the main study, respondents were self-selecting. For heuristic evaluation peers and experts in the fields of study were purposefully selected to ensure that their evaluation is based on skills and knowledge of the domains. This will give credibility to the recommendations.

5.3 DESIGNING THE DATA COLLECTION

This section presents the process followed in designing the data collection.

5.3.1 Research instruments used

Semi-structured interviews, policy document reviews and a self-administered online survey were used to conduct the case study research.

5.3.2 Designing of the instruments

5.3.2.1 Semi-structured interviews

Two sets of questions were compiled to guide the research. The questions were formulated to gain a richer understanding of phenomena to be studied and to ascertain if there is indeed a problem. The target participants were five technical (group 1) and five non-technical (group 2) employees. Questions were open-ended, so as to allow respondents to provide insight into the situation.

5.3.2.2 Survey questionnaire

An online survey questionnaire was designed to collect data, based on the findings of the pilot study and it is found in Appendix A1. The questionnaire was used to address end user issues in Information Security focusing on end user application programs. The aim was to establish security problems resulting from inadequate support for end users in using security features

embedded in the application programs they use daily. Data was collected about security awareness, experience with security interaction, usage and problems associated with the use or lack of application security. The raw data is confidential and was used to assess the extent of a need to improve the end user's interaction with security features on their computers. To determine the appropriate questions, the Research Question 1 of the study was broken into sections reflecting the main pillars of the theoretical framework. Standard end user information security questionnaires, such as the one by University of Wisconsin (2008), were adapted for use. The questions were mainly open-ended to allow for rich qualitative data to be gathered. Respondents were encouraged to think and to express themselves freely. Closed questions were also included to enable quick answers and to increase the number of responses as the tool was long. They also allowed for quick reflection on the state of affairs. Where closed questions were employed in most cases other responses were included to allow for capturing responses that may have been missed by the list provided. To improve the responses, rated ranked (e.g. Likert scale), matrix and multiple selection questions were also used. Three- and five-point Likert scales were used to capture attitudes, frequency and technology usage.

The online survey is quick and inexpensive to administer. It also saves time in analysis as the data can be analysed electronically using statistical tools. A survey was conducted in order to understand how the community handles security issues related to electronic information. To get an overall understanding of information security problems resulting from inadequate end user support, questions focused on ensuring that information was gathered about end users' knowledge (awareness) of the security threats they are exposed to when they connect to networks, as well as security solutions; awareness of computer security policies in the organisation; experiences with security interaction; security technology/solutions usage among the community members; the programs used for primary tasks at work/ job; knowledge of security features embedded in application programs and operating systems; and behaviour towards security alerts.

The information was gathered to give a holistic picture of the issues impacting on user experiences with security.

5.4 PREPARATION FOR THE DATA COLLECTION

From the pilot studies it was evident that end users and technical staff members had different views regarding security challenges in the organisation. It was necessary to ensure that the participants in the research reflected both parties. The first step towards objective data collection was to identify the participants for the pretesting and validation of the survey, followed by the identification of participants to participate in the survey. Once the participants were identified, then a pilot (exploratory) study was conducted to explore and establish the security awareness, behaviour, experience and attitudes towards EUP security features in the case site, using each data gathering method so that problematic areas could be uncovered and corrected.The pre-testparticipats did not participate in the main survey as they had already responded and their responses were used to improve the tool for the main study.

5.4.1 Permission to carry out research

A letter seeking permission from the Bureau of Computer Services (BCS) was written to the network and security manager of the case site. Upon receipt of the signed approval (see Appendix A2), a cover letter was designed for the survey explaining the purpose of the study, as well as establishing rules for confidentiality and ethical conduct. The cover letter is provided in Appendix A3. A pilot study was then conducted to establish the existence of the problem through semi-structured interviews, and policy document reviews; and the survey tool was pretested.

5.4.2 Pilot studies: Data collection method 1: semi-structured interviews

As presented in Section 1.2.2, semi-structured interviews (see Appendix A4) were carried out with five technical (group 1) and five non-technical (group 2) employees to understand the attitude of the population representatives towards security features and the support given or received. Two sets of six questions were presented to the two groups. The findings reflected are presented in Section 1.2.2. After the pilot study, a policy document review was carried out, which is presented in the next section.

5.4.3 Data collection method 2: Policy document reviews

Organisational policy documents available on the staff intranet were reviewed and compared to the templates from SANs. The policies conform to the standard templates. The analysis of documentation at the case site revealed a list of policies for implementation. The following policies exist at the case site:

1. Acceptable ICT use describes the acceptable use of ICT equipment in the institution to guarantee that the organization is safe from “risks including virus attacks, compromise of network systems and services, disclosure of confidential information and legal issues”, which is meant for all ICT users in the organization. It is meant to spell out acceptable use of ICT resources (Polytechnic of Namibia, 2008).
2. Password Policy, defining practice for constructing and safeguarding strong passwords, and the frequency of change.
3. Remote access, for all employees accessing the institution’s network off-campus with either a company-owned or personal computer, laptop, workstation or mobile device for work-related activities.
4. Virtual Private Network (VPN) which prescribes how to use Remote Access through IPsec or L2TP VPN connections to the organization’s corporate network.
5. Wireless communication that prohibits connecting to the organization’s networks through unsafe mobile communication devices and specifies that access can only be approved by the ICT department.

Having established the existence of standard policy documents it became necessary to understand why an organisation having the right infrastructure, human resources and policies to drive their process is challenged with security issues. An imperial study was carried out, which process is described in Section 5.4. Before conducting the actual study the survey tool was pretested and validated.

5.4.4 Survey validation

The questionnaire was sent to professionals for validation. It was checked for achieving the objective of the data collection, convergence, language and its appropriateness as a tool. A survey question's validity is established by how well it measures the phenomenon on which it is intended to gather data. Validity can either be convergent or divergent; it can be measured through comparing answers to questions measuring the same aspect (convergent), or by comparing the answer to the same participant's response to an exact opposite question. Convergence was tested on the objective and question relatedness. Feedback was used to refine the tool. The feedback included the following:

1. “As a general comment, the fact you are carrying out a pilot study must have a single, clean statement to which all the questions relevantly apply. I am struggling a bit to find it, as well as to relate some questions to the overall picture; perhaps they are treated further in the questionnaire (I did not go too far beyond the first page).” This was addressed in the introduction.
2. I just took a tour through your questionnaire:
    1. “You certainly will need to put in ranges for age and department requests. Psychologically you get a truer answer if the respondent can "hide" behind a range than when s/he is put on the spot to reveal an exact number.” This was addressed on employment period; however, the age was additional information. Hence, the strata were not important even in the analysis of findings. It was captured to understand how the individual responded. In case of departments, it was difficult to do so as there were many departments in a faculty and respondents generally use preference to identify their departments; hence, they were at liberty to state their department. Then classification would be done relative to institutional groupings.
    2. “Wherever you have "Other", it would be a great idea to actually capture the detail. You get a wealth of surprising information with this option.” This was rectified by providing space to add specifics.
    3. “I notice you had a request that has an option for "ALL THE ABOVE". I believe it would be good if all the other boxes are either unchecked automatically, or checked automatically to confirm this selection. Otherwise your analysis might throw out some interesting errors at analysis.” This was rectified.
    4. Where the respondent has responded "NO", do not insist on getting their "YES" version in a follow-up question. You will need to examine the question links. Hide/unhide of options is a good idea in this case, just as you would on a paper-based questionnaire (e.g. if answer is "NO" proceed to Question n, or skip Question n).

5.4.5 Data collection method 3: Survey pre-test

Pretesting helps to determine the strengths and weaknesses of the survey with regard to wording, order and question format. Pretesting also determines if the questionnaire is understandable (participating) and the relevance of the choice of analysis (undeclared).

Once the validation feedback was incorporated, the survey tool was pre-tested with seven users. A cover letter explaining the purpose of the study and the survey link were distributed via email. The recipients of the pre-test email comprised one professor in Human Computer Interaction, two Doctors in Communication, and four lecturers in the school of Information Technology (IT). The choice of the participants was to ensure that field-specific content is validated, and that the flow and language issues are also exposed. Using the responses gathered the tool was fine-tuned and deployed to all population members (670) using a broadcast email to distribute the link. The pre-test helped to pick up any typos, and highlighted ambiguity in the wording of the questions.

5.5 DATA COLLECTION

5.5.1 Data collection plan

The focus of the study was established by forming questions about the problem to be investigated and determining a purpose for the study. The problem to be studied addressed Research Question one. Seven main questions were developed and each was further broken down to collect as much information to understand the phenomena in context. A questionnaire was developed using E Surveys Pro. The study objectives and cover letter were publicised to all staff members in the institution through a broadcast email together with a link to the online survey. Data was collected only from those who willingly chose to respond, over a period of 21 days. The survey tool was open for 21 days during which 58 annonymous participants described in table 5-2 completed the survey.

5.5.2 Data collected

Semi-structured interviews collected end users' and technical support opinions about information security in the organisation. Thetechnical voice brings out how the technology experts view the problem at hand and their proposed solutions, on the other hand the typical user will explain why they behave in the manner they do. Understanding the user presents an opportunity to understand how intervention can be designed and implemented in the case site. On the other hand, policy

document reviews collected information about the policies in existence and their compliance to international standards.

5.5.2.1 Demographics

The participants entered their age, gender, department and their employment period in the organisation. The gender distribution is shown in Table 5-1.

Table 5-1: Participants' representation by gender

Gender	Total
Female	25
Male	33
Total Respondents	58

Table 5-2 shows the department affiliation of participants to the departments constituting an academic institution.

Table 5-2: Respondents' affiliation

Department	Participants (n=58)
School of Information Technology	18
School Of Business Management	8
School of Communication, Media & Legal Studies	2
School of Engineering	2
School of Natural Resources	3
School of Health and Applied Sciences	1
Computer Services	2
Centre of Open and Long life Learning	4
Centre of Teaching and Learning	1
Centre of Entrepreneurial Development	1
Registrar	1
Library	1
Auxiliary Services	1
Payroll, Finance and Accounting	3
Human Resources	2

Namibian German Logistics	1
Campus Security	1

58 responses were collected from personnel in the departments shown in Table 5-2. The affiliation speaks to the computer user expertise.

The employment period in the organisation speaks to the culture; the longer you stay the more you conform to the norms and practices in your environment. Table 5-3 is a summary of respondents' tenure.

Table 5-3: Participants' employment period in the case site

Employment period	Total respondents
0- 6 Months	4
6-12 Months	3
1 Year +	6
2 Years +	10
3 Years +	11
4 Years +	3
5 Years +	21

The results are based on inductive analysis of security threats and solution awareness; user behaviour while interacting with security features; their attitudes and feelings towards security; and security policies in place. The interpretations are supported with extracts of actual responses.

Critical literature review has established that Information security problems are largely due to users' behaviour towards security features and perceptions of program security. To evaluate UX, a hierarchical approach was employed as presented by Colabro (2012). It presents three stages as follows:

The first stage is **general knowledge** that is used to provide a basic sense of end user program security usage. It gives an overview of whether end users are aware of security threats and solutions at their disposal. Tools for this include usage analysis and in this study a survey was used to gather the information. Next, data was collected on user behaviour.

Stage two is **understanding** user behaviour, which is used to determine what users are doing and where a problem exists (are they using security features or not?). This can be used to establish why users are not using security features. The tool used for this is a case study where an online survey (using E Surveys Pro) was deployed to a population of 670 end users and the sample respondents (53) were analysed for patterns. Once the behaviour is known, the next step is to measure UX associated with the features.

Stage three is **influencing the users** by determining if a security feature is compelling through measuring the emotion associated with the feature. The researcher used a survey to find out how the users think and feel about embedded security features in the programs they use. This is followed by recommended mechanisms to ensure positive experiences for users while using the security features.Table 5-4 is a summary of the findings of a survey conducted in line with stages one and two.

Table 5-4: Summary of survey findings

Survey question	Findings	Survey Section
Your knowledge of the security threats you are exposed to when you connect to the network.	Users not aware of the security threat associated with disclosure of passwords	8.8
	Participants are aware of their email program handling spam	8.1
	Participants are generally aware of security threats they are exposed to.	2.1
	Shows that the participants are aware of whether they were compromised or not, yet the prior question indicates low awareness. This is contradictory- likely that they do not know what they are saying	2.2
	92% Of participants did not receive any computer security training	4.1
Your awareness of computer security policies in the organisation.	At most 29% of the participants know of the password policy followed by internet with 23%, then general computer usage with 21% and wireless has 13%. Ironically, every staff member has a computer for their work; all academic staff also have a laptop which connects both to the wired and wireless networks in the organisation.	4.2-3
	Participants are not aware of the existence of the policies; hence, the policy application is not exercised. 45% got the awareness from BCS, but it was by signing the document not reading through and understanding it.	
	Users do not adhere to institutional policies on general computer usage. All problems must be reported to BCS; however 41% of the participants depend on friends and the internet.	8.6

Survey question	Findings	Survey Section
Your experiences with security interaction.	Majority of participants acknowledge having received security alerts A large number of users feel that the notifications are disruptive, irritating and annoying -63%, while only 30% feel positively about it They appreciate system feedback with regard to their actions Participants are generally negative about acting on displayed security alerts/ notification (58%). Despite their appreciation of the feedback, they still have negative feelings towards the display of notifications which require their action. Participants are usually busy with core duties, they feel they are either not responsible for security; or it's their computer therefore must be responsible, or they are obliged to act and yet others feel they should protect their information. Participants regard alerts as being informative, warning, reminders or notifications	6.1 6.3 6.4 6.5 6.6 3.5
Security technology/ solutions usage among the community members.	Participants display a great deal of knowledge about password usage and handling. Participants are aware of the need for different passwords for accessing different resources. Participants know that passwords should not be written down Only a few of the participants share passwords with their colleagues.	7.1-4 & 5.2 7.1 7.2 & 7.3 7.4
The programs you are using for primary tasks at work/ job.	The popularity of programs among participants is best with email client at 100%; next are web browser at 92%; then word processors (86%); next is ITS at 68%; followed by spreadsheets and presentation software both at 62%. The document readers are at 50%; the rest are seldom used. The computer is mainly used as a tool for communication, then research, internet browsing, teaching, internet banking, and administration. A diversity of email clients are in use, contrary to expectations. Social networking programs are used, especially Facebook, followed the professional network LinkedIn	5.1 9.8 8.5 5.4;3.13 &3.14
Your knowledge of security features embedded in your Application Programs and Operating System.	46% of respondents configured program security options 68% of participants are aware of the existence of spam filters in their email programs Very few participants are aware of encryption mechanisms for emails (e.g. digital signature, certificates same status)	5.2 8.1 8.4
How you behave towards security alerts.	Majority of participants make informed decisions. They actually read through before making a choice; however, 18% ignore or just click to	6.2

Survey question	Findings	Survey Section
	get rid of the message.Password controlled access is better secured; however, they are prone to social engineering as they (40%) trust anyone who claims to be technical support with their login credentials.	8.8
	Participants are cautious about email attachments although they trust emails from unknown sources.	8.2 & 8.3
	When confronted with a computer problem, end users trust the insecure Internet (29%) for help, and 12.5 trust their colleagues for a solution. This exposes them to internal threats as well as to hackers.	8.6
	Users generally do not update their programs as often as required with 27% only doing it often; 53% when prompted by the software or technician; and 18.5% sometimes or never update.	3.1
	7.7% of the participants disable security programs from running on their PC; however, the majority let them run.	3.3
	The majority of respondents do not disable alerts from running (83%)	
	The respondents who disable alerts do so because they feel negatively about it. Even among those who say it is their responsibility, there are still others who disable the alerts as shown in the error handling cross tab.	3.4 3.5
	Many end users allow add-on to run from the Internet, coupled with the fact that most of them have administrative rights on their machines. This poses a great security risk.	3.6
	Mixed feelings among respondents; however, most will move away from the site and do nothing about it. A few would contact the webmaster. The patterns show that they are aware of restrictions to visit certain sites. If genuine, they act on it.	3.7
	The majority of respondents feel it is appropriate for organisations to block some sites	3.8
	86% of respondents can install programs on their machines.	
	Many of the respondents download and install software from the Internet and do not use secure connections [cross tab]	3.9 3.10 &11

The findings have established that many factors, such as lack of knowledge, awareness, prioritizing their work targets and misconceptions regarding security threats affect end user experience with security. This, in turn, influences how they do/ not secure their information. The next section will focus on knowledge of security threat; question 1 of the survey.

5.5.2.2 Knowledge of security threats

The users are generally aware of the information security threats that they are exposed to. The survey showed awareness as high as 94% for hacking and as low as 30% for social engineering, as depicted in Figure 5-1.

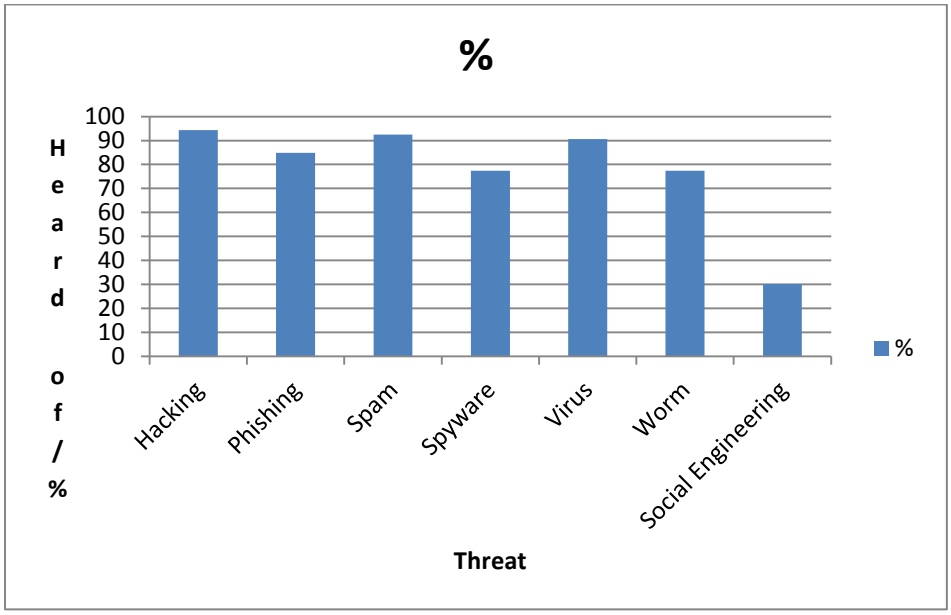


Figure 5-1: End user awareness of security threats

End users have heard about security threats; however, 13% of the respondents knew that they had been hacked; 24% were not sure and the remaining 63% knew they had not been hacked. It is quite likely that they do not understand how hacking is carried out; hence, they cannot detect it. Of the 92% who are aware of what spam is, 64% know that they have been victims of spam and explain how it happened to them. In most cases it was through unknown email, one responded testifies that "I received some unsolicited and unwanted mails into my inbox. Viruses affected my computers and these mainly came from the students' memory sticks I opened on my computers and attachments on certain documents that were sent to me by people I do not know." The second part of the response speaks to how computers are usually infected due to downloads of infected or malicious files, and sharing of usb devices. The same trend is observed for all the other threats, as shown in Table 5-5.

Table 5-5: UX with security threats

Have you ever been a victim of:	Yes	% Yes	No	% No	Do not know	% Do not know	Total responses
Hacking	7	14	32	63	12	24	51
Phishing	10	19	30	58	12	23	52
Spam	32	64	13	26	5	10	50
Spyware	16	35	21	46	9	20	46
Virus	43	83	6	12	3	6	52
Worm	24	48	15	30	11	22	50
Social Engineering	3	6	17	36	27	57	47

Further enquiry showed that 68% of the users are aware of their email programs handling spam. With this level of awareness, it is tempting to assume that they know how to handle their emails well; however. 44% would open emails from unfamiliar sources and 29% open all attachments they receive. When confronted with a problem, 40% will disclose their passwords to the "support" personnel. This support can be offered telephonically or using remote desktop managers. They do not have a perception of the implications of disclosing their passwords. This indicates that there is no user training on information security, as confirmed by 92% of the participants shown in Figure 5-2.

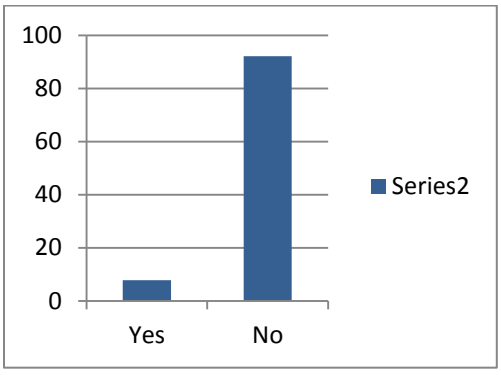


Figure 5-2: Security training

5.5.2.3 Security Policy awareness

The findings show that, at most, 29% of the participants know of the policies that exist in the organisation. 29% know about the password policy, followed by Internet at 23%, general computer usage at 21% and wireless hat13%. Ironically, every staff member has a computer for

their work, all academic staff members also have a laptop that connects both to the wired and wireless networks in the organisation. Of those who know about policies, 45% learnt about them from the right office and the rest from a colleague or friend.There is a need for the organisation to train up users on policies, the organisation has no awreness programs in place. This shows that users are not aware of the existence and proper usage of the policies; hence, the application of policies within the organisation is not there. The findings reflect that there is no adherence to the policies, as shown by the behaviour when confronted with a computer-related problem. The official way is to seek help from the Computer Services, yet Figure 5-3 shows that about 42% seek it from the most untrusted sources of information such as the Internet, friend or colleague.

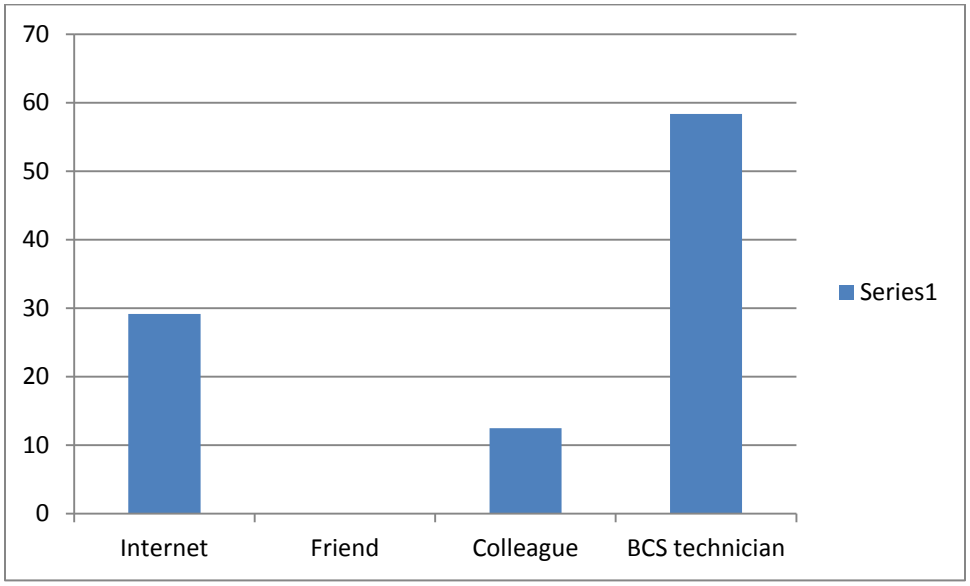


Figure 5-3: Source of help

5.5.2.4 User experience with security interaction

The end users acknowledge receiving security alerts and appreciate receiving system feedback. They feel it is "informative" and serves "To inform me when a program needs to be updated or if a virus has been detected". However, they have negative feelings (63%) for notifications, especially when required to act on them (58%). When asked "Updates prompt you with a notification to install every 3 hours if the expiry date is more than 24 hours away, and hourly if within 24 hours. How do you feel about this?" most of the responses were "irritated", "annoyed", "this is too often" and time consuming among others. For instance one responded to question 3 said it should be the technician's responsibility: "I have lots of work to consider thinking about

security"; and yet another said "there is a department respossible for that". Among those who are irritated their response is "Because most the time it happens while I am very busy and it seems like it stops me from working effectively." or "Because you are busy with some task and then you need to stop everything to adress the message.". Figure 5-4 shows some of the feelings they experience with the interactions, such as disruptive, irritated and annoyed. The majority have negative feelings; however, 41% feel it is their responsibility as reflected in their responses: "I am responsible for the computer and the information thereon so I need to take the messages seriously".

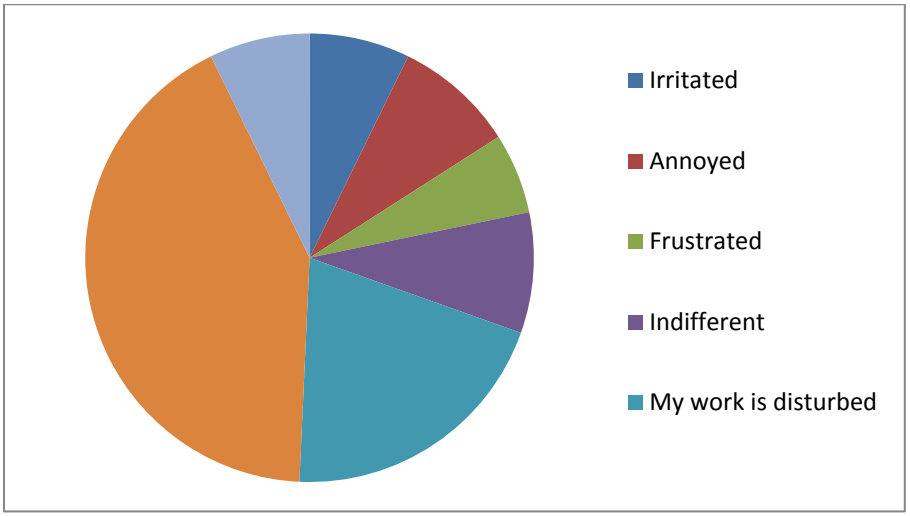


Figure 5-4: Feelings towards acting on security messages

5.5.2.5 Security technology/Solution Usage

Table 5-6 shows the frequency of using different types of security technology. Anti-viruses and passwords are the most used protection mechanism with a presence of 71%, followed by firewalls. Updates are only implemented by 33% and this means the systems are left vulnerable to current and new attacks targeting known vulnerabilities. The most shocking realisation is the fact that end users do not back up their information, with only 22% doing it.

Table 5-6: Frequency of using security technology

	%Not at all	%Rarely	% Sometimes	% Often	%Always
Antivirus	2	0	11	15	72
Firewall	11	8	11	21	49
Antimalware	47	13	11	9	19
IDS	53	15	15	8	9
Passwords	6	0	6	17	72
Patches	47	13	13	8	19
Updates	9	13	17	26	34
Backup	9	9	32	26	23
Encryption	45	23	13	11	8

5.5.2.6 Frequently used programs

These are the application programs used to perform daily tasks by end users on their computers. Table 5-7 is a presentation of programs used in the case site.

Table 5-7: Program usage

Program	% Always	% Sometimes	% Not at all
Word processor	86	10	4
Spreadsheets	62	36	2
Presentation	62	36	2
Graphics	20	56	24
Project management	4	30	66
Document readers	50	28	22
Database management	18	42	40
Email	100	0	0
Web browsers	92	6	2
ITS	68	30	2
Other	26	52	22

In his study, it was established that the most popular programs are email clients at 100%, web browsers at 92%, word processors at 86%, ITS at 68%, followed by spreadsheets and presentation software, both at 62%, document readers are at 50%, and the rest are seldom used, as shown in Table 5-7.

These findings reflect on the Furnell et al. (2005) findings where they identified the same programs as popular. SANS (2009), SANS (2011) and (TippingPoint, 2009) have also rated the popularity and security exploitation of application programs, they found MS Word and Adobe among the popularly exploited (due to late or no patching) and most popular end user programs.

Table 5-8 shows that the computer is mainly used as a tool for communication (emails, chats and instant messging), then for research, internet browsing, teaching, internet banking, and administration, in that order.

Table 5-8: Uses of the computer

	% Always	% Sometime	% Not At All
Communication	87	13	0
Research	85	15	0
Teaching	57	38	4
Administration	51	47	2
Internet Browsing	83	17	0
Internet banking	53	30	17
Downloads	40	34	26
Music, Skype, Games	17	51	32
Other	17	47	36

A diversity of email clients are in use, contrary to expectations. The case under study uses CommuniGate pro (Pronto webmail) for business; however, Figure 5-5 shows many others including Windows Live mail. 9% of users selected others and specified Pronto; therefore, there are 17 respondents using CommuniGate = 35%. 65% do not know that they use Pronto on a daily basis.

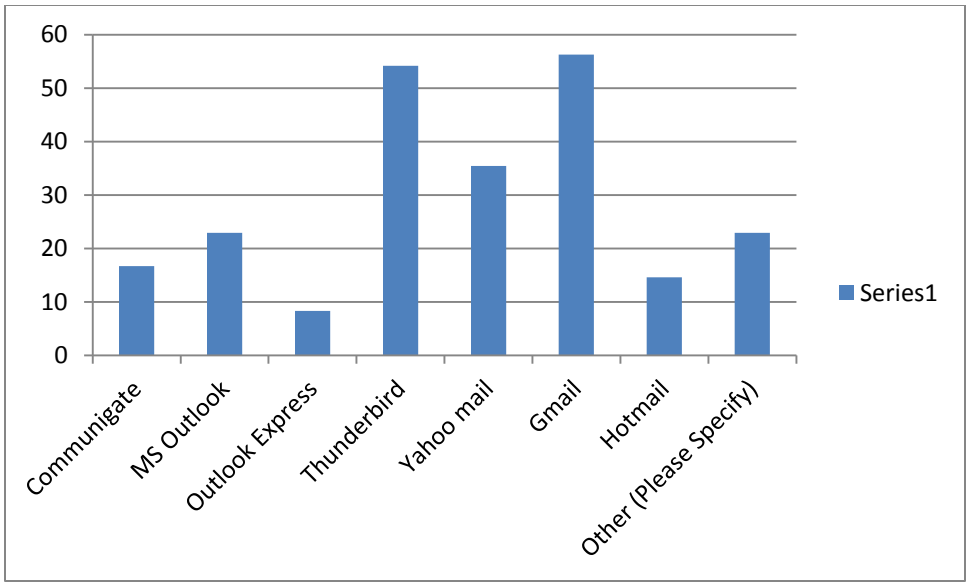


Figure 5-5: Email clients

Social networking programs, especially Facebook (74%), followed by the professional network LinkedIn (65%), are popular among the respondents. They share a wide range of information with their contacts including photos, as well as personal and professional information. One respondend shares: "Usually information about workshops and conferences (professional) and family events (social)." What are the risks associated with this behaviour?

5.5.2.7 Embedded security feature knowledge

Only 46% of respondents have configured security options in their programs. The idea of encrypting information sent out via emails is unknown with only 4% using the feature. Embedded security is not being used as often as necessary. This presents an easy target for cybercriminals.

5.5.2.8 Behaviour towards security interactions

Behaviour is affected by organisational culture, as highlighted in Chapter 4. To understand the user behaviour in depth, the organisational basic assumptions, values and beliefs plus artefacts on information security need to be understood. User behaviour is influenced by many factors such as lack of knowledge, prioritizing their work targets and misconceptions regarding security threats (Herzog & Shahmehri, 2007). The survey has confirmed the same facts. A majority make informed decisions; they actually read through before making a choice; however, 18% ignore or

just click in order to get rid of the message. When it comes to passwords, they seem to be more careful although they are susceptible to social engineering attacks. They easily trust (40%) anyone who seems to be offering claims to be technical support with their login credentials. They are cautious about email attachments although they trust emails from unknown sources.

When confronted with a computer problem end users trust the insecure Internet (29%) for help, and 12.5% trust their colleagues for a solution. This exposes them to internal threats, as well as to hackers. End users generally do not update their programs as often as required with 27% doing it often; 53% when prompted by the software or technician; 18.5% sometimes or never. In a quest to address this, end users were joined to a domain and some software updates have been automated from a central server. The effectiveness; however, depends on the user logging onto the domain instead of onto their local PC.

7.7% disable security programs from running on their PC; 17% disable alerts; however, the majority let them run. Those who disable alerts do so because they feel negative about them. They feel irritated, annoyed, frustrated, and indifferent. Their work is being disrupted or it is the technician's responsibility to deal with the alerts; however, even those who claim it is their responsibility to look after their security, are users who disable the alerts. This is contradicting their feelings- there is no alignment of behaviour to feelings, even among those who say it is their responsibility. There are still others who disable the alerts as shown in Table 5-9, a crosstab of two tables.

Table 5-9: Feelings about notifications and alerts handling

	Feelings about notifications							
		Irritated	**Annoyed**	**Frustrated**	**Indifferent**	**Work is disturbed**	**My responsibility**	**Technician's responsibility**
Alert Disabling	Yes	8	8	8	8	25	17	25
	No	7	9	5	9	19	47	4

There are mixed feelings about web sensing, when a message is displayed notifying them that the page they are trying to access has been blocked by the organisation. Most will navigate away from the site and do nothing about it. According to one responded, they "move away from the site and navigate to a site that is similar and is not blocked". A few would contact the web

master, i.e. “If it is content that is work related then I'll contact the Systems Administrators to unblock it”. The patterns show that they are aware of restrictions to visit certain sites; if genuine, they act on it. However, the majority feels it is appropriate for organisations to block some sites.

Of concern also is the fact that many end users allow add-ons to run on their computers from the internet, coupled with the fact that most of them have administrative rights (86%) on their machines. This poses a great security risk. Viruses and other malicious software can be executed remotely on their machines. They download and install software from the internet and do not use secure connections. 60% trust browser auto completion, which may lead to a hacker’s site without their knowing it. Based on this, there is a need to address the education aspect which targets basic assumptions in order to influence cognitive behaviour. The findings reflect that the end users belong to mode 1 and 2 of the information security behaviour modes framework by Alfawaz, Nelson, & Mohannak, (2010). As indicated by Schein (2004) a longitudinal in-depth study will reveal unconscious assumptions that shape Polytechnic of Namibia’s culture. The information gathered from the survey is not sufficient to help understand what drives user behaviour.

5.5.3 Summary of findings

The findings have established that many factors, such as lack of knowledge, lack of awareness, prioritizing their work and misconceptions regarding security threats affect the end user’s experience with security. Poor security-related decisions and behaviour with an overall negative experience with InfoSec are common, as programs are left vulnerable to exploitation by cyber criminals. As an intervention user training on computer security and security policies in place are recommended.

Improving information security means enhancing user attitudes towards security features in the programs they use for their work. To improve user experience with security the users must be aware of security threats, solutions/features; they must know the benefits of using the features and must interact with the security features.

Literature on the problem domain established that user attributes such as awareness (of security issues, solutions and policies), attitude/perception; and EUPSF usability are among the key factors affecting UX with security feature interactions. It can be noted that awareness of security

issues, solutions and policies forms the basis of end user feelings while interacting with technology (EUPSF). The feelings shape attitude and perceptions which, in turn, influence user experience with end user program security features. User experience influences and is influenced by technology usability and organisational culture, both of which determine user behaviour. Poor usability results in negative feelings and user experience. This means that the user will not use the technology (behave negatively) and therefore, there is no information security. On the other hand, positive feelings and user experiences result in technology usage (positive behaviour) and ultimately, in information security. Organisational culture is not depicted in the theoretical framework as it is outside the scope of the study; it is a field of its own and will need a thesis of its own. The theoretical framework in Figure 5-6 is a product of consolidating the outcomes of literature studies presented in Chapters 3 and 4 and the findings from the case studies conducted. It covers the human factors, user experience, usable security, user behaviour and information security knowledge domains.

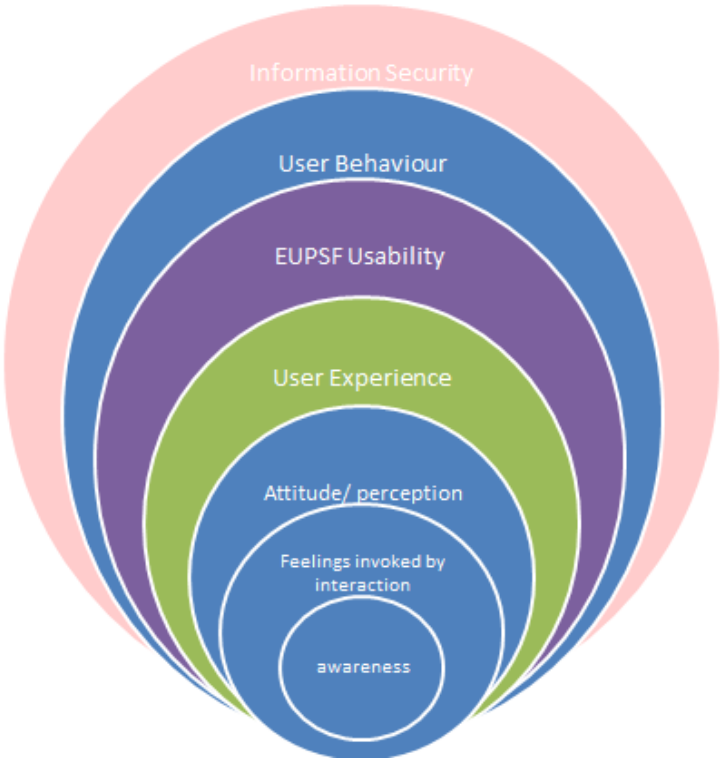


Figure 5-6: Theoretical framework

As the aim of the study was to determine the factors influencing UX with embedded security features, the following are the key factors were identified:

1. Awareness of security threats, solutions, policies
2. Feelings invoked by interaction
3. Usability of the security feature
4. End user's attitudes and perceptions of the security task
5. Prior user experience
6. User behaviour with security features
7. Organisational security culture

End users will be able to interact with embedded features only if they feel good about them (the security will be usable). In the light of all these factors, it is recommend that users be educated on security threats, solutions, policies and secure behaviour as a way of influencing future experience and organisational security culture.

The next section will present a security awareness approach.

5.5.4 Security awareness approach

As established by the survey results, there is no awareness program in the case site. Following the awareness model by Spitzner (2012), the focus is first placed on compliance, which focuses on the implementation of standards, promoting user awareness and change through an awareness program tailored for the organizational needs; on long-term sustainment, which addresses how to improve the organizational posture continually through unceasing improvement; and on metrics, which measure the effectiveness of the awareness program. Security metric development guidelines were already presented in Section 4.8.2 and were used to guide the security awareness approach that consists of two primary stages.

Stage 1: Compliance with standards

Based on the information gathered on end users' knowledge of the security threats; awareness of security policies in the organization; security technology solution awareness and usage; and behaviour towards security interaction, it is evident that the organisation complies with ISO security standards on security management (ISO 27000 series). Good and relevant policies are in place and are implemented from the administrative side.

Stage 2: Promoting awareness and change

To promote awareness and change, there is a need for a motivation or baseline to be established. It should not be based on what everyone else is doing. Since the survey has shown that knowledge of security threats and solutions, security policy awareness, security technology usage and negative user perceptions and behaviour with regard to security, there is a need to develop a reference metric for the organisation to evaluate the security awareness baseline.

Based on the results presented in the previous section, metrics were developed using the Goal-Question method presented in Section 4.8.2. For instance, the metric is user behaviour. The question asked is: how do you behave when confronted with a security dialogue? The goal is to measure user behaviour with security dialogue boxes.

There are seven steps involved in developing a security metrics program, as presented in Section 4.8.2. In this research the focus is on the first three presented, namely:

1. Define the metrics program objectives and goals.
2. The objective is to identify metrics that evidently lead to improving user interaction with security features.
3. The goals are to have a metrics program founded on improving awareness in the studied organization; the metrics should be communicated effectively to all stakeholders (end users and technical staff). Decide on metrics to be produced. A bottom-up approach was adopted from Payne (2006) and is shown in Table 5-10.

Table 5-10: Bottom-up approach employed for analysis of results

Bottom-Up Approach	
Identify measurements that can be collected for this process.	The percentage of users unaware of security policies in the organization; security threats and solutions; the ratio of users who behave securely.
Define metrics that can be generated from the measurements.	The number of users aware of security policies; threats and solutions from the last dated survey, as well as system and antivirus logs; the number of end users who behave securely and the number of successful security breaches logged by the security monitoring software.
Determine the association between resulting metrics and established objectives of the overall security program.	The metrics should inform the development of an awareness program that can increase the security policy, as well as threat and solution awareness among end users.

5.5.4.1 Findings on knowledge of policies

The policies are well articulated; however, the effect of their implementation on user experience is unknown. Users barely know the security policies; hence, they do not use them as expected, as shown in the findings. Table 5-11 shows responses to the question: "To what extent do you know these policies? (1 is not at all and 5 is very well)"

Table 5-11: Knowledge of policies

	1	2	3	4	5	Response Total
Password	11	2	11	12	15	51
Wireless	14	9	14	7	7	51
General computer usage	13	4	14	9	11	51
Internet	14	4	9	12	12	51

Extent 5 is the minimum risk ranked at one (1) and Extent 1 shows a major risk ranked at five (5). Generally the policy knowledge risk is moderate (3.04) because the participants identify with average to low knowledge on policies in the organization. Interviewed practical computer lecturers and IT laboratory technicians indicated that students are not assigned enough memory on campus servers and end user PCs to store their data and information. Their computer user accounts are mandatory. Typically mandatory user profiles delete user information/data on log off. This scenario encourages the use of removable devices among students as they share and save materials with peers or lecturers. From the survey results, 81% of the respondents use USB sticks to exchange information. Network sharing, Google docs and Drop Box are not common. From a security point of view, emails and memory sticks are good paths for spreading viruses. As witnessed in the computer laboratories, malicious code is the major breach and extends to the staff intranet. Malicious code mainly comprises virus infections with an 85% occurrence; the remaining 15% are Trojan horses, as captured in anti-virus logs.

Using risk factor assignment to questions on security policies awareness, Table 5-12 presents the calculated awareness risk values for different policies in the organization.

Table 5-12: Calculated risk rating for security policy awareness

Policy	Average risk value	Awareness risk value	Risk rating
Password	171/51= 3.35	50	Elevated
Wireless	137/51=2.69	40	Elevated
General computer usage	154/51=3.02	45	Elevated
Internet	157/51= 3.08	46	Elevated
Overall	3.04	45	Elevated

5.5.4.2 Security Policy Awareness

The organisation has policy awareness ranging between 13% and 29% for the surveyed policies. Figure 5-7 shows how those knowledgeable about policies learnt about them. Interestingly, among those who responded some were not aware of the policies, yet they responded positively.

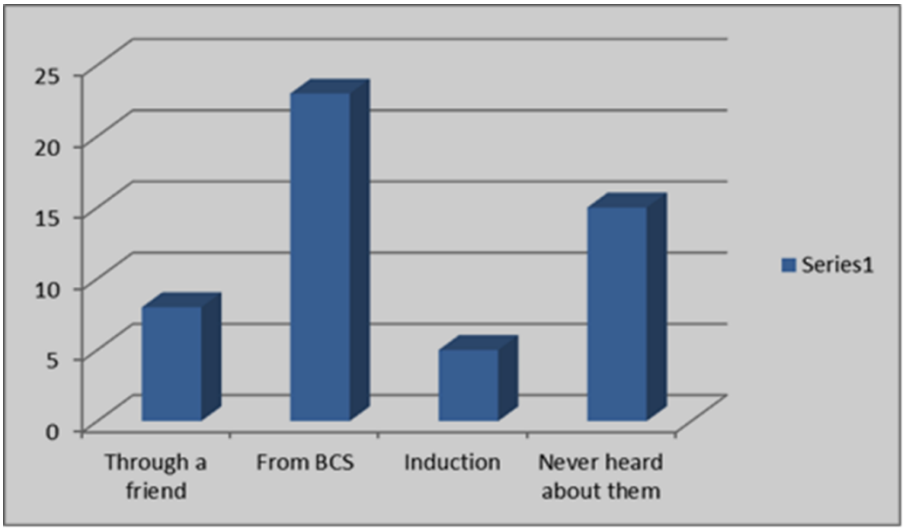


Figure 5-7: Where users learn about security policies

Evidently, there is a need for user education with regard to organisational policy awareness, to ensure that those who know about their existence obtain the knowledge from the right sources. Consequently, there is no policy compliance as witnessed by user behaviour when confronted with computer issues. The policy compliant way to respond is to seek assistance from the IT support department; yet approximately 42% source assistance from less secure sources, including Internet, friends or colleagues, as shown in Figure 5-3. The general computer usage policy stipulates that all sensitive information must be encrypted; however, only 15% of the respondents

make use of the technology. User behaviour with regard to policies presents a major risk to the organisation's security.

5.5.4.3 Security metrics vs awareness

Based on the findings, there is a need to develop and implement a security awareness program in the case site. Currently, the organization is at level 1 of the security awareness roadmap as described by SANS (2012). The security awareness roadmap has different levels with the first level stated as non-existent, followed by compliance- focused. The third level speaks to promoting awareness and change that, in turn, leads to long-term sustainment, which is evaluated by metrics at the final level 5. Figure 5-8 is the security awareness roadmap.

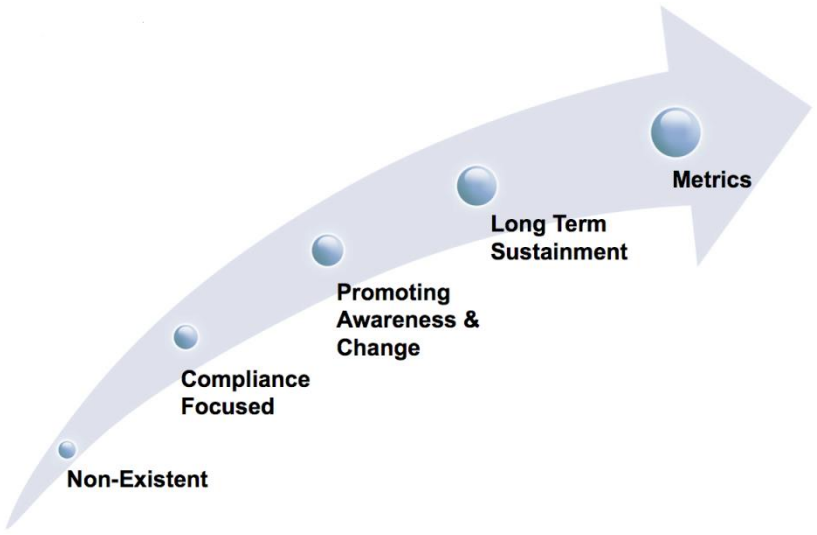


Figure 5-8: Security awareness roadmap adopted from SANS (2012)

The stages of implementing a security awareness program involve establishing a baseline, acting and then evaluating the impact. Based on the findings, specific security awareness metrics for establishing the baseline are proposed (see Table 5-13).

Table 5-13 Security awareness metrics

Metric	What is measured?	How it is measured	Details
Awareness survey	Number of users who: know about security policies; use policies; violate policies; know about security threats, breaches and solutions	Survey Tracking user behaviour related to access policies	To what extent do users know/ understand or use security tools, features or policies?
User behaviour	Number of users who behave negatively with regard to security	Survey	What is the current status at the case site?
Computer infections	How many computers are infected?	Antivirus logs	Are the infection behaviours related?

For one to be able to design effective security awareness there is a need to carry out an awareness survey to establish a baseline. The baseline will serve as a reference or comparison point for measuring the impact of awareness campaigns. It is important to know what computer users already know. The findings reflect the absence of user training. This is a direct measure of metric 1.

The second metric from Table 5-13 is user behaviour, which should align to policy and best practices. The number of users behaving negatively can inform an organization of the need to draw up a security awareness plan. It is important to have an understanding of what users do with the ICT resources. Thirdly, there is a need to know the computer attacks that affect the users, their frequency and how these impact on information and technology usage. Analysis of antivirus and system logs can reflect on the most prevalent infections, the sources, when they occurred and the number of devices affected. The source of infection and the propagation mechanisms of breaches can inform what needs to be changed in terms of behaviour and know-how.

5.6 CASE STUDY VALIDATION

As already said in Section 2.4.7, the quality of a case study can be demonstrated. There can also be a demonstration of the validity, and reliability of the process. Four tests for case study quality were applied, as shown in Table 5-14.

Table 5-14: Case study validity based on Yin, (2009)

Test	Case study tactic	Phase when tactic was applied
Construct validity	1. Framework components- literature review, semi-structured interviews and surveys were used as sources of evidence 2. Awareness metrics- literature survey, survey, document (anti-virus logs, policy documents) review 3. Heuristic evaluation - literature review, program documentation, survey, security task analysis were used as sources of evidence	Data collection Data collection Data collection
Internal validity	Pattern matching/ coding Explanation building Address rival explanations (contradictions in the data) Use logic models	Through literature review, where applicable, or document review. For metric calculation
External validity	Theory (the organisation is a representative case- single case selected. The embedded cases are programs typically common in the single-case contexts)	The six steps of conducting a case study were followed; hence, this was addressed in the process.
Reliability	Used the six-step case study protocol to conduct the study.	Data collection can be repeated using the same tools and process. However, results vary as they are influenced by human and contextual factors, as well as by technological evolution.

5.7 SUMMARY

This chapter presented the case study that was conducted. The pilot case study explored the extent of the UX problem, and the main case study validated the extent of the problem and the components of the theoretical framework. The pilot and empirical studies have highlighted problems that face end users while using computers to process, store and transmit personal or organisational information. It was established that end users do not behave as expected and there is a need for action to reduce security risks in the organisation. User education on policies and their requirements, as well as security best practices, were some of the issues identified. The end user attitudes toward security are not positive. The findings reflect a scenario where there is a support mechanism from the organisation. It can be inferred that in scenarios where individuals are not supported they experience more negative encounters with security.

The pilot and empirical studies have addressed stage 1 and 2 of Colabro's (2012) three ways of influencing UX. Based on the findings it became necessary to address stage 3. Stage 3 involves influencing the users by determining if a security feature is compelling, through measuring the emotion associated with the feature. Firstly, the proposed awareness metrics are used to evaluate

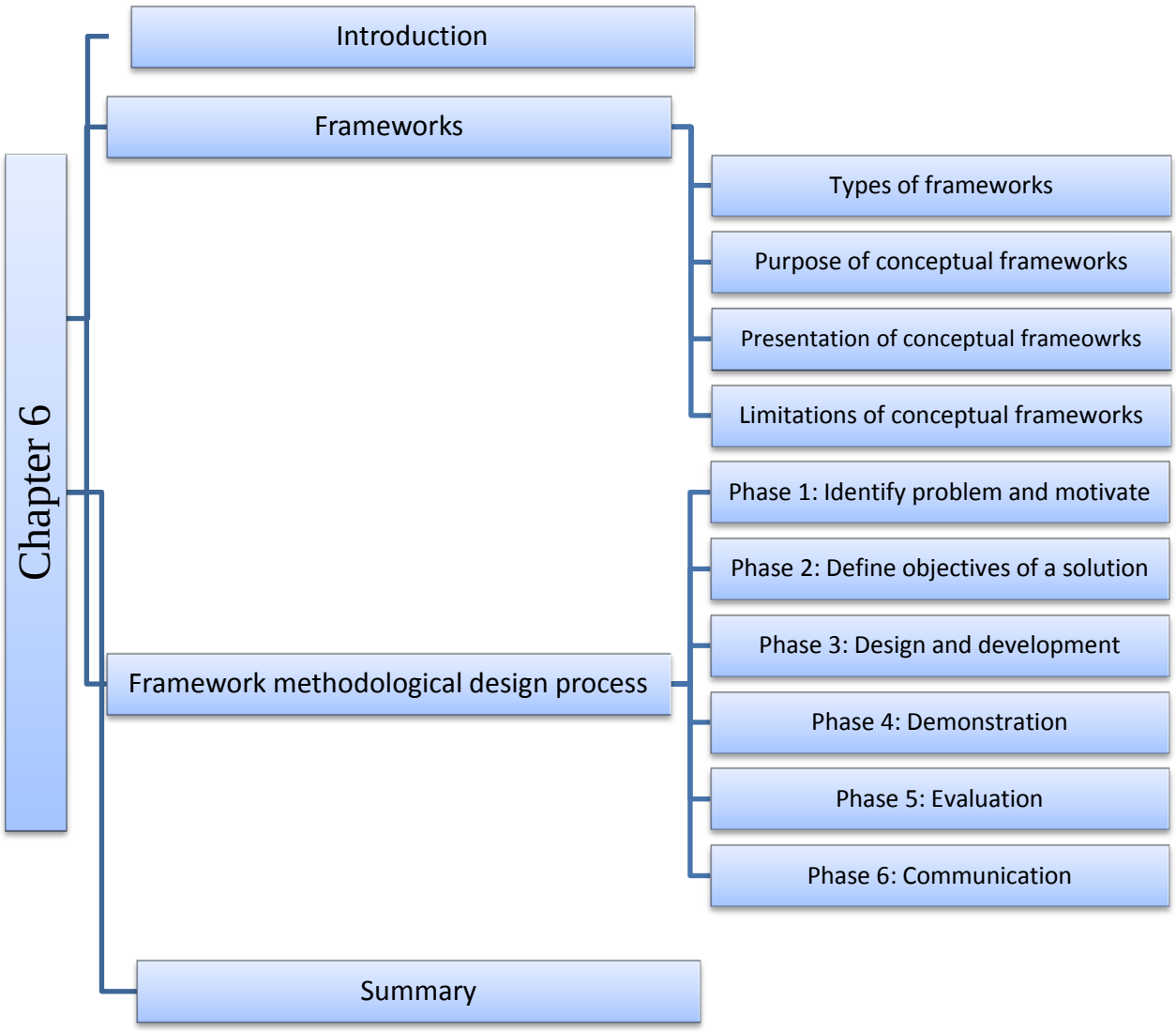
security status and to establish a baseline. Three metrics were identified: user awareness survey, user behaviour and computer infection levels. Secondly, USec and UX heuristics should be identified and exposed to peers and experts to perform cognitive walkthroughs and to evaluate each heuristic against a checklist of items. The HE is meant to give a general perspective of the usability and UX of features in selected applications, as well as to validate the UX criteria for usable security features. After this, mechanisms are recommended to ensure positive experiences for users while using the security features. The mechanisms will ensure that end user experience factors identified in this study are addressed. This, is turn, will ensure that end users interact correctly while having a positive experience with embbeded security features.

The findings reflect negative user experience (measured by usability, emotions and attitudes), moderate EUP usability and a need to train end users on security features. These are in line with the theoretical framework; hence, they can inform the developments of a framework in Chapter 6.

CHAPTER 6: FRAMEWORK DESIGN

6.1 INTRODUCTION

The previous chapter presented the empirical research that was conducted and its outcomes. This chapter sets out the process that was used to develop the framework following the outline in the chapter map. Section 6.2 describes the different types of frameworks and motivates for the specific framework type that is presented in this chapter. Section 6.3 presents the framework methodological design process. The subsequent sections describe and follow the design process outlined in Section 6.3. Therefore Section 6.3.1 presents stage 1 of design science research namely the problem identification. Section 6.3.3.1 discusses construct identification and validation in 6.3.3.2. Section 6.3.3.3 discusses the relationships among the components identified in the previous sections and proposes the EUPSFUX conceptual framework in Section 6.3.3.4. Section 6.3.4 presents the actual framework in action. The framework is then evaluated in Section 6.3.5. Finally, the summary is presented in Section 6.4.



6.2 FRAMEWORKS

Frameworks can provide the structure upon which the systems can be built. Generally, frameworks are operational in nature and provide structure: a detailed description of how to implement, create or manage a programme or process. They are characteristically principles-based and open to continuous improvement. As a result, frameworks usually rely on subsidiary standards to 'make it happen', and they are further complemented by implementation guides and other detailed documents (von Roessing, 2010).

6.2.1 Types of frameworks and definitions

Several types of frameworks exist and, besides the conceptual type, two others are common, namely: practical and theoretical frameworks (Eisenhart, 1991). A theoretical or conceptual framework is a set of views on how certain concepts or phenomena are linked and why it is so (Sekaran & Bougie, 2009). Table 6-1 summarises the different types of framework identified.

Table 6-1: Summary of framework types

Type	**Description**
Practical	A practical framework is determined by accumulated knowledge of practitioners and administrators, the results of preceding research and perspectives from a public view (Eisenhart, 1991; Lester, 2005).
Theoretical	Represents one's beliefs on how certain variables or concepts are related in a model and explanations of the phenomena (Sekaran & Bougie, 2009).
Conceptual	"explains, either graphically or in narrative form, the main things to be studied—the key factors, concepts, or variables—and the presumed relationships among them" (Miles and Huberman 1994; p. 18)
Others	Structural, visual and social frameworks.

According to Tomhave (2005), "A framework is a fundamental construct that defines assumptions, concepts, values, and practices, and that includes guidance for implementing itself". A conceptual framework is a reusable **construct** that implements a generic solution to a generalized problem (Lethbridge and Laganiere, 2005). It is a set of views on how certain concepts or phenomena are linked and why it is so (Sekaran & Bougie, 2009). Borgatti (1999) defines it as a collection of interrelated concepts, like a theory but not necessarily as well worked-out. These definitions were important in this thesis as they provided the platform to come up with the proposed EUPSFUX framework. The following coined definition will be adopted for the EUPSFUX framework: **A conceptual framework is a reusable construct that defines assumptions, concepts, values, and practices for implementing a generic solution about a phenomenon, including guidance for implementing and evaluating itself (Borgatti, 1999; Lethbridge & Laganiere, 2005; Tomhave, 2005; Sekaran & Bougie, 2009).**

Using the definition, the researcher was able to identify the major components of the framework and the key stakeholders to be involved in the framework design. Stakeholders are important in focusing our evaluation as they will be evaluated in the case of end users or will use the framework to evaluate UX (in the case of IT, UX and IS practitioners). As established in Section 1.1, security is about the human factor; hence, the realistic collection of realities about product use is rarely possible without end users, especially when it comes to interactive products (Pentti Routio, 2007). Figure 6-1 shows the composition of a framework.

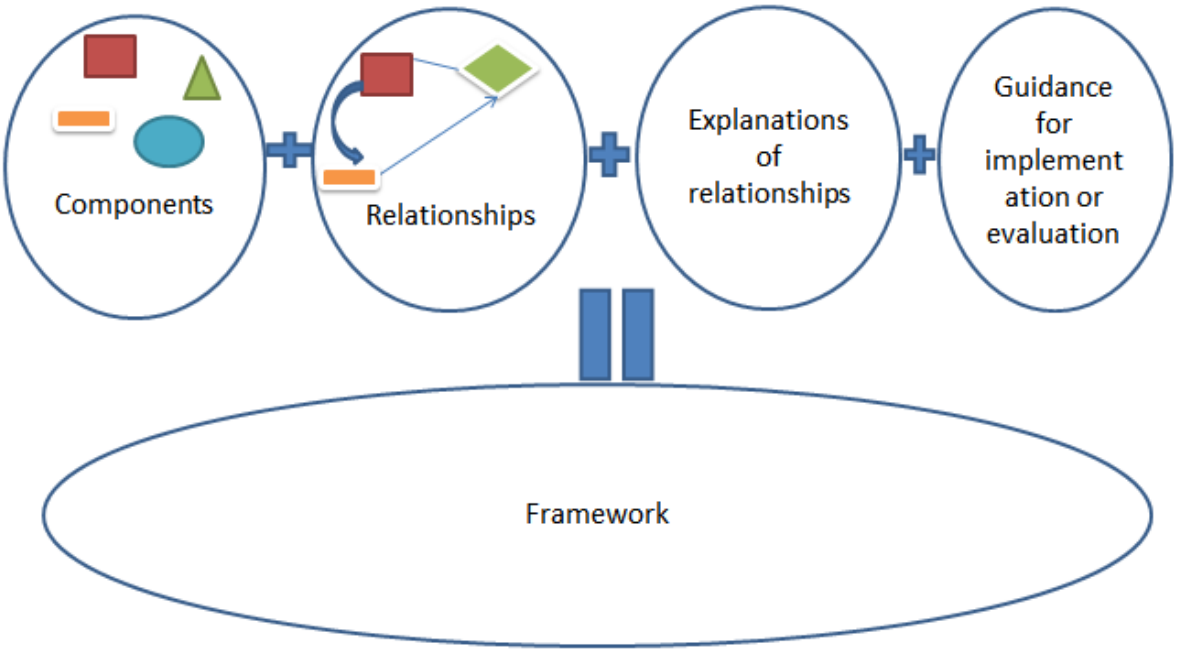


Figure 6-1: Composition of a framework

A conceptual framework can explain concepts and suggest relationships among concepts in a study; make a context available for interpreting research findings; explain observations through mathematics, models or statistics (Miles & Huberman 1994).

Coming up with a conceptual framework involves defining the concepts and developing a conceptual model of your theory explaining the connections among the variables (Sekaran & Bougie, 2009). A concept is made up of a number of components and is defined by them (Jabareen, 2009). According to Miles and Huberman (1994), a conceptual framework describes, explicitly or in a story, the core aspects to be studied, the "key factors, concepts, or variables—

and the presumed relationships among them" (p. 18). It offers an interpretive approach to shared truth (Jabareen, 2009). Table 6-2 presents the different components of conceptual frameworks, descriptions and the literature source.

Table 6-2: Component descriptions

Component	Description	Source(s)
Variables/ concepts/ key factors	Theoretical/ abstract or empirical/descriptive Elements of participating variable	Sekaran & Bougie,2009 ; Tomhave, 2005; Lethbridge & Laganiere, 2005; Miles and Huberman.1994
Relationships	Conceptual model describing relationships and direction of the relationships	Sekaran & Bougie ,2009 ; Tomhave, 2005; Lethbridge & Laganiere, 2005; Miles and Huberman ,1994
Explanation of relationships/ Processes	Explanation of why these relationships exist. A schematic diagram of the theoretical framework	Sekaran & Bougie ,2009; Lethbridge & Laganiere, 2005
Guidance	Specific guidance for using and implementing the framework	Tomhave, 2005; Lethbridge & Laganiere, 2005

The next sections will discuss types, purpose, presentation and limitations of conceptual frameworks.

6.2.2 Types of conceptual frameworks

Types of conceptual frameworks include working hypotheses; descriptive categories; practical ideal types; models of operations research, and formal hypotheses (Oates, 2006; Shields & Rangarajan, 2013). According to Miles and Huberman (1994, p. 18 and 54), they can be: rudimentary or elaborate; theory driven or commonsensical; descriptive or causal. They can be represented as a model (schematic (boxes and arrows) or mathematical/ statistical (with letters, numbers and mathematical symbols)). A conceptual paradigm is a preliminary design before validation (empirical investigation) (Nalzaro, 2012; Paditar, 2014). According to Vaughan (2008), they can be process frameworks showing how actions move from start to end, usually

used to address the ‘how?’ question; or they can be content frameworks where clear variables are identified and linked by relationships, to answer the ‘why?’ question.

As this research aims to develop a descriptive conceptual framework, the components (concepts) will be identified; relations will be modelled and the outcome will be tested for evaluating the UX of EUPSF successfully. The concepts, in this case, are the topics that address user experience with security features interactions. These are UX, USec and user awareness. Section 6.2.2 presents the purpose of conceptual frameworks.

6.2.3 Purpose of conceptual frameworks

According to Nalzaro (2012) and Paditar (2014), the purpose of conceptual frameworks is to:

1. Clarify concepts and propose relationships among concepts in a study
2. Provide a context for interpreting study findings
3. Explain observations

According to Vaughan, (2008), they offer investigators:

1. The capacity to move past accounts of ‘what’ to justifications of ‘why’ and ‘how’.
2. A way of defining a reference point that influences the definition and interpretation of the data that is gathered from the research question.
3. A clarifying tool for choosing suitable research questions and associated data collection methods.
4. A locus point/structure for the review of the literature, methodology and results.
5. The delineation of the research.

In this research the conceptual framework will serve as a tool for clarifying concepts, and their relationships, and will provide a context for interpreting research findings. Next, conceptual framework presentation strategies are discussed.

6.2.4 Presentation of conceptual frameworks

Conceptual frameworks can be presented using: flow charts; tree diagrams; shape-based diagrams – triangles, concentric circles, overlapping circles; mind maps or soft systems (Vaughan, 2008). In this research the choice is to use shape-based diagrams.

6.2.5 Limitations of conceptual frameworks

The framework is prejudiced by the know-how and understanding of the researcher – initial bias. After developing the theoretical framework, it guides the investigator's thoughts and may influence choices regarding what to consider and what to disregard – on-going bias. This can be addressed through iteration of evaluation and development.

6.2.6 Conclusion

For the purpose of this study, a descriptive conceptual framework is deemed appropriate. The following section will present the descriptive conceptual framework (EUPSFUX) methodological design process.

6.3 EUPSFUX METHODOLOGICAL DESIGN PROCESS

Based on the different methodologies presented in Chapter 2, as well as on the literature review in Chapters 3 and 4, an application of the framework development process is presented in this section. The composition of end user experience measurement framework has four critical components (Ireland, 2014). These components guarantee that UX metrics measure key factors of end users' product experience influencing secure UX. The components are: end users' needs understanding; knowledge of what is key to end users; identifying metrics to measure success for your environment (organisation and product) around the contextual themes; and end user success metrics identification for the themes (Ireland, 2014).

The success of the research depends on having a full appreciation of end users and their interaction with security features. User studies were used to gather information that can help in understanding the users in context. Factors affecting end users were established and compared to literature. The proposed theoretical framework was thus validated by the findings. To evaluate end user program features UX, information security and end user programs' evaluation methods will be used jointly to reflect the intertwinning of the two fields. EUPSFs interact with end users; hence, their design follows user-centred program and security design principles in information systems. This is worth considering in coming up with the framework. Figure 6-2 shows how the phases of the design science research and problem based research were combined to come up with the framework design methodological approach. Stages involved at every point are depicted in the diagram, based on several literature sources and will be explained in detail when the phase is addressed.

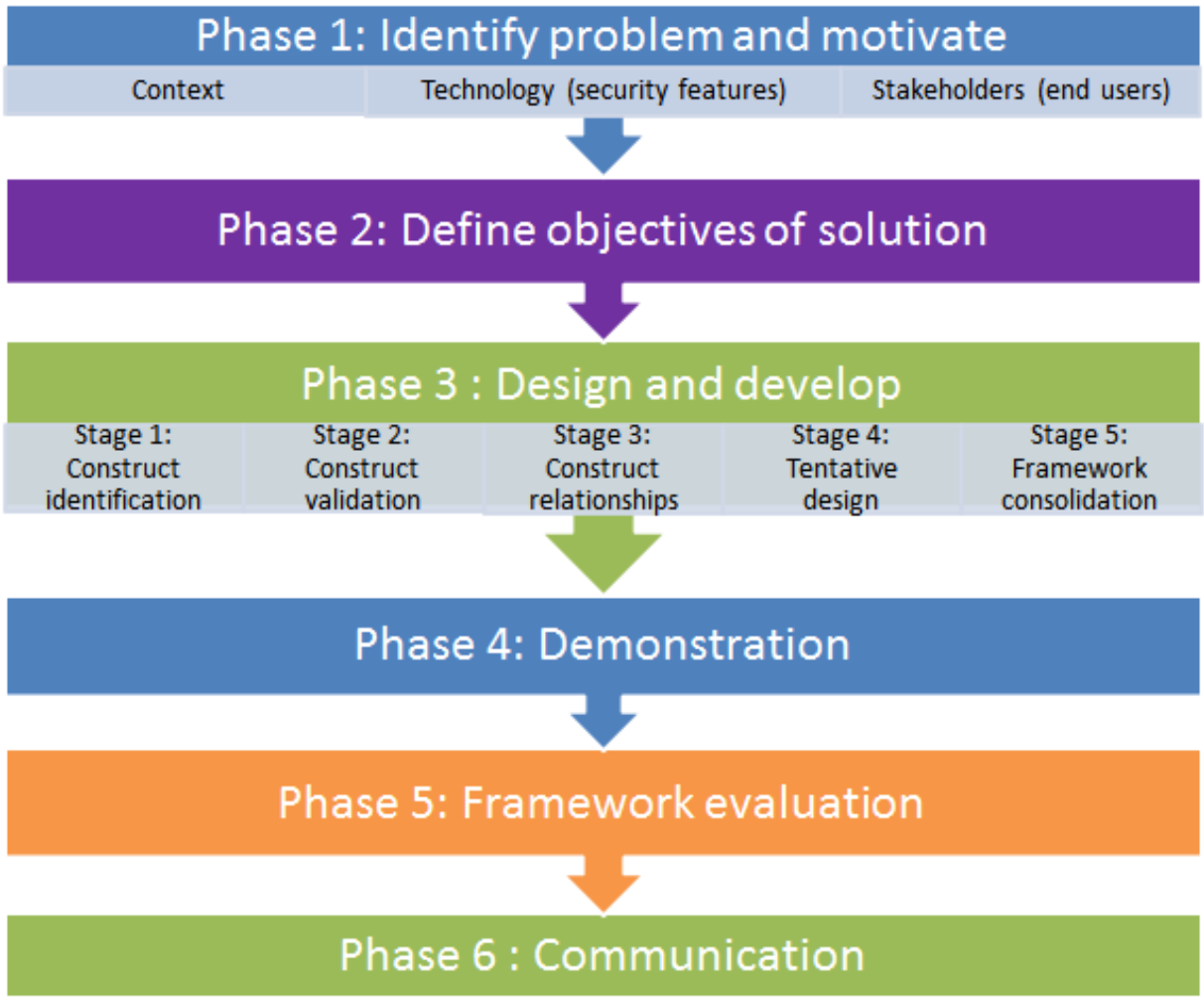


Figure 6-2: EUPSFUX methodological design process

The next section will present the application of the process phase by phase.

6.3.1 Phase 1- Identify problem and motivate

This section focuses on the area highlighted in Figure 6-3. As explained in Chapter 2, design science research methodology Phase 1, in line with problem based research cycle, stages 1 and 2, was used to define the problem that will be addressed by the framework. The question that motivated the framework development, as presented in Section 1.4 is - "**How can UX evaluation criteria and metrics necessary for end user program security features be constituted into a framework?** To answer this question a supporting question was answered first: **What are the factors influencing user experience with security features?**

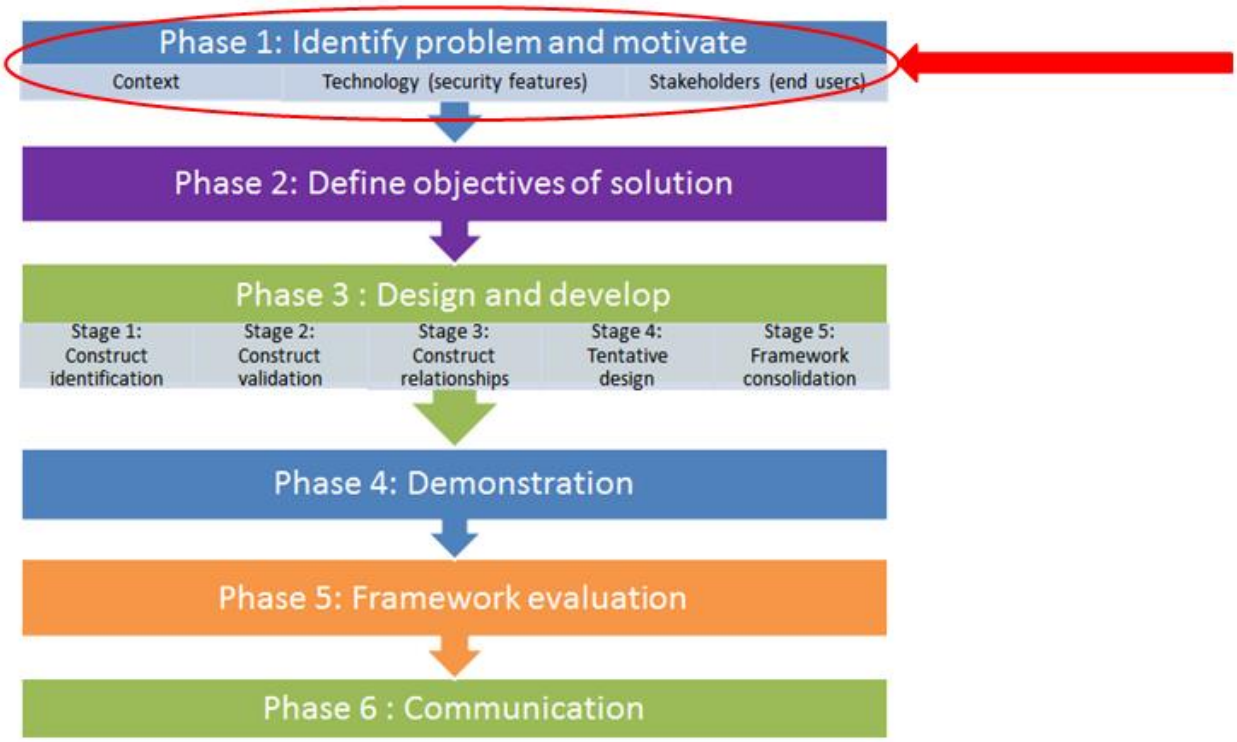


Figure 6-3: Phase 1 of the EUPSFUX methodological process

Literature reviews were conducted and documented in Chapters 3 and 4. This enabled the identification of a broad set of factors which can affect user experience in the studied organisation. The identified factors influenced the design of data collection tools for user studies and the analysis of the collected data presented in Chapter 5, as they formed the theoretical framework underpinning the study. The factors identified are: **user awareness of security threats and solution; policy awareness and implementation; feelings invoked by interaction, prior user experience, end user's attitudes and perceptions of the security task; security technology usage; as well as user behaviour with security features, and technology acceptance.** They led to the definition of the problem. The findings reflected the extent of the problem and motivated the need for an artefact.

User awareness was identified as the basis to addressing the problem, as it forms the core of how the end users perceive and respond to interaction with security features. In order to address the lack of awareness problem it is necessary for the case site to design an awareness program.

However, before an intervention can be done, a well-defined criterion for evaluating the awareness levels was necessary.

Upon identifying the significance of user awareness, it then became necessary to identify metrics that can evaluate adequately the user awareness levels in context. A bottom-up approach was used and the resultant metrics are: an awareness survey, user behaviour and computer infections. To delineate the research and align it to the study objectives, focus was placed on awareness surveys as they influence behaviour and, consequently, the number of computer infections witnessed. IT Technical staff administered the awareness survey to end users. The purpose of the awareness survey was to collect data on the factors influencing user experience of end user interaction with end user program security features.

In the context of the study, stakeholders were critical as they are the people who influence the security culture of any organisation. In this study, the identified major stakeholders are end users, information security experts, IT team (support/administrators/help desk) and UX experts, respectively. The relevance of artefact is with respect to stakeholders. Technically, these are the experts who plan, design, implement, operate, evaluate and manage the EUPSF.

However, this is a subset of many users who can be involved including security and UX designers, programmers, system and security administrators (Zurko & Simon, 1996). Preliminary data was collected by surveying the stakeholders to establish the extent of the problem (exploratory study or/and actual study). The collected data was analysed qualitatively by coding and pattern matching and analysis. The findings were validated using literature as reference point in Chapter 5. The problem identification process is presented in more detail in Chapters 1 and 5, where the actual study is described.

The output of phase 1 is a statement of the problem as indicated in Chapter 1, Section 1.3:

> There is a lack of user experience evaluation criteria (metrics) to assess the user experience of end user interaction with embedded security features in end user programs.

6.3.2 Phase 2 - Define objectives of a solution

The problem sets out the objective and questions of the study in line with stage 2 of the problem based research cycle, by Ellis and Levy (2010) and Phase 2 of DSRM process model by Peffers,

et al. (2008). The EUPSFUX framework will provide an evaluation platform, the evaluation criteria and the guidance to implement it and thus to solve the identified problem. The research objectives were defined upon identifying the research problem presented in Sections 1.4 and 2.4.8. Phase 2 is highlighted in Figure 6-4.

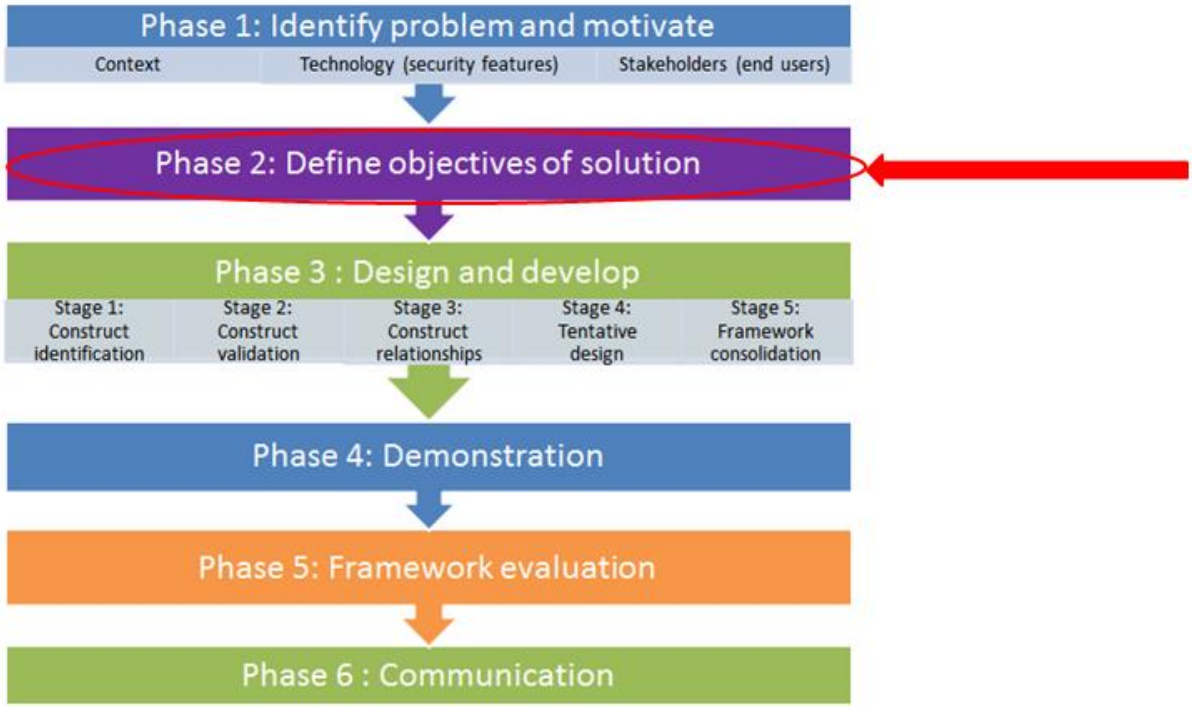


Figure 6-4: Phase 2 of the EUPSFUX methodological approach

Primary objective:

This research aims to design a framework that can be used to evaluate the user experiences (UX) of interacting with end program security features from a user's perspective.

Specific objectives:

1. To measure the state of UX with end user programs' embedded security features.
2. To determine the suitable security criteria/ methods that can be used to evaluate UX of end user program security features.
3. To determine UX metrics/evaluation criteria can be used to determine the UX of end user program security features.
4. To determine the components and requirements of end user programs' security features' UX and use them to develop the EUPSFUX framework.

6.3.3 Phase 3 - Design and development

The research design was presented in Chapter 2 and can be summarised. The research followed an interpretive approach using inductive reasoning and qualitative methods in a case study setup. Qualitative data collection instruments employed include questionnaires, structured interviews and literature surveys. The questionnaire had open ended questions to collect end users' opinions.

Literature established the different fields and domains that are vital to the problem under study. These are human (end user) factors, user experience, usable security (EUPSF), user behaviour and information security. The outcomes of Chapters 3 and 4 were brought together to define the theoretical framework presented in Section 5.5.3. To validate the importance of the components of the theoretical framework, an empirical study was conducted and presented in Chapter 5. The empirical study identified seven factors presented in Section 6.3.1. The identified factors are elements of the five domains in the theoretical framework. However, the **user behaviour and organisational culture** will not be addressed. Policies were reviewed for compliance with standards and to validate their presence in the organisation as they are vital to influencing human behaviour and shaping the security culture of the organisation. However, there was no in-depth analysis to evaluate their overall impact on UX as an individual aspect. The following sections will resent the stages of Phase 3 as highlighted in Figure 6-5.

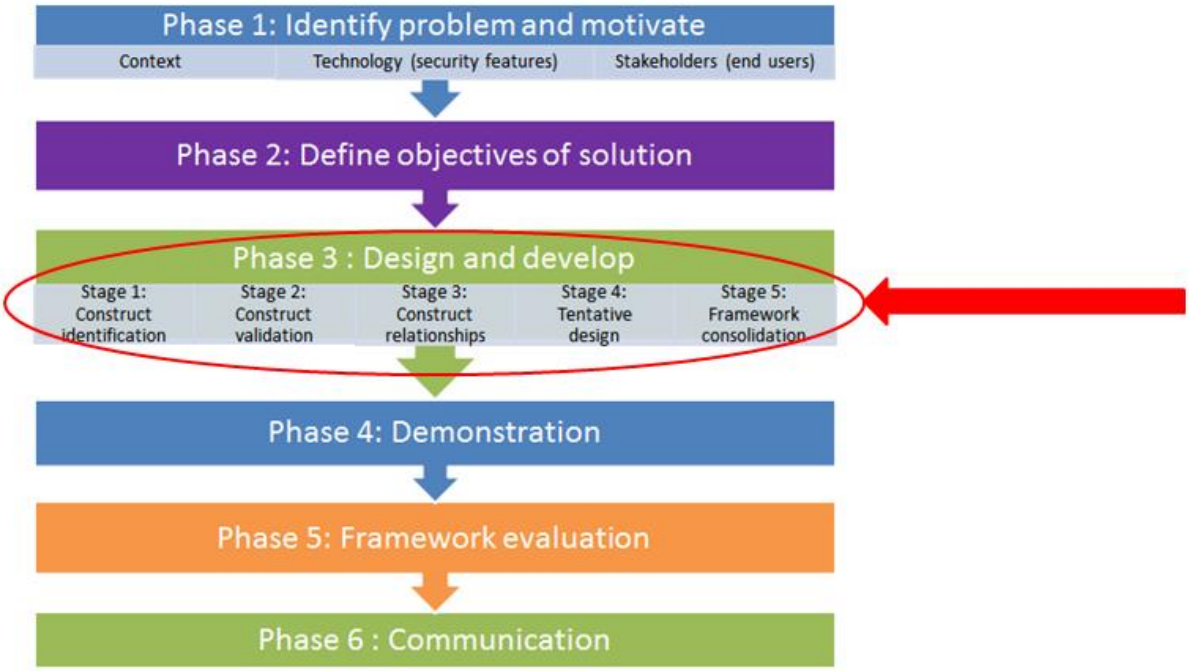


Figure 6-5: Phase 3 of the EUPSFUX methodological approach

6.3.3.1 Phase 3 - Stage 1: Construct identification

Stage 1 of the problem based research cycle is the research methodology. This provides a roadmap of how the research will be conducted (Ellis & Levy, 2008). The outputs of this phase are constructs and associated components for the framework, as shown in Table 6-3.

The concepts/ constructs in this case are the topics which address user experience with security features interactions, as identified in Chapters 3 and 4 and presented in the theoretical framework in Section 5.5.3. The chosen components were based on the analysis of the empirical data, as well as on the theoretical framework. As there are many dimensions to UX, for the purpose of this research focus will only be on interaction of UX components. These are UX factors, EUPSF (the product under study), the USec aspect of information security (InfoSec) and the user awareness aspect of the end user characteristics. The framework is composed of components of EUPSFUX evaluation, criteria, validation tools, stakeholders and their roles and an implementation procedure. Table 6-3 is a listing of identified components in this research study.

Table 6-3: Constructs and components

Construct	Components
End user (human) characteristics	**Awareness,** knowledge Anticipation/ expectation Motivation Prior experience Emotions, attitudes, perception, priorities, Goals, behaviour
EUPSF (Usable security)	SF characteristics (complex, rare, unpredictable, usability) EUP characteristics InfoSec goals: confidentiality, integrity, availability, privacy, non-repudiation
UX factors (components)	End user characteristics Context (EUP, organization, academic) Product (EUPSF)
InfoSec/Context	Where (work, personal), what (program in use), culture, policies, secure information, InfoSec goals

6.3.3.2 Phase 3 - Stage 2: Construct validation

Stage 2 comprises using findings and literature to validate the constructed framework. This section describes how each of the constructs was validated during the development of the EUPSFUX.

Construct: End User (EU) characteristics

As presented in Chapter 2, an end user is the person who uses the program to complete a task and can be any one of the stakeholders. The person has attributes such as: motivation, expectations, perceptions, priorities, goals, prior knowledge or awareness, prior experience, emotions, attitudes and behaviour. These are characteristics of a human user that can be influenced by the environment or by the product in use. Figure 6-6 is a pictorial representation of the construct and its characteristics. Awareness and user experience feature as the most prominent characteristics and, as such, will be addressed by the framework:

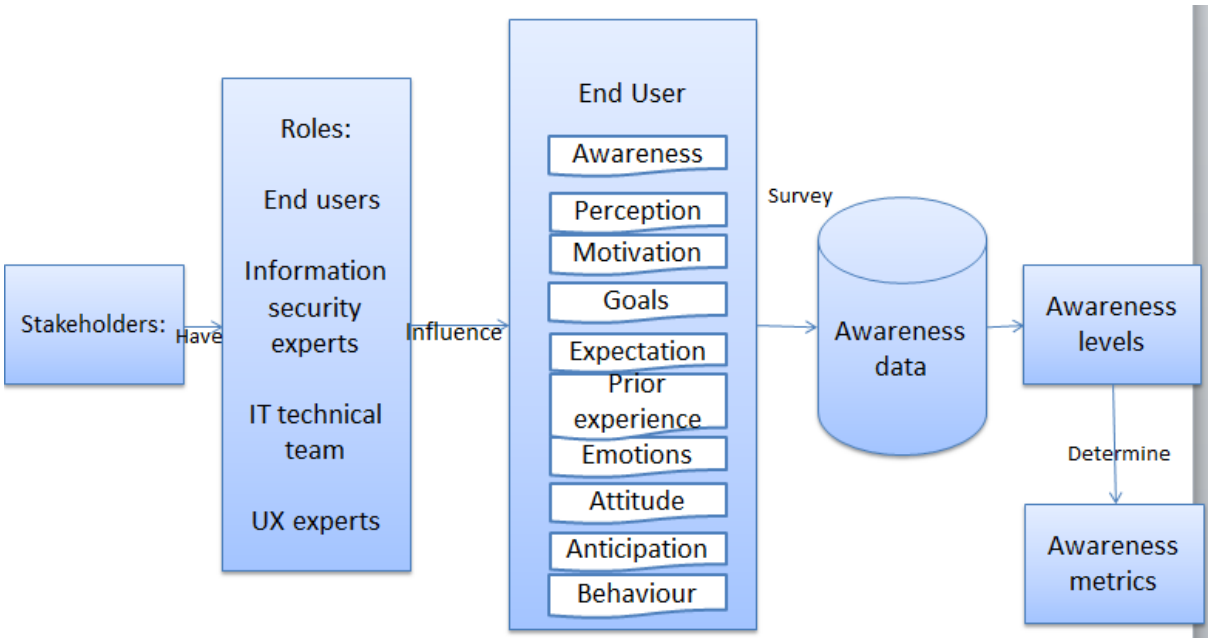


Figure 6-6: End user characteristics

Several instruments were used in the research; hence, limitations will be integral to different methods contributing to overall limitations. Questionnaires (to gather end user awareness of security threats and solutions, security policies and secure behaviour; feelings with interaction as well) and heuristic evaluation by stakeholders of end user program security features were applied. The questionnaire survey identified awareness and lack of knowledge as critical elements of human factors, followed by perceptions and attitudes. Perceptions and attitudes can be addressed more as UX factors even though they are human attributes. In this section a motivation for why user awareness is important as a component is presented.

User awareness of security threats scored highly except for social engineering, which was known to only 13% of the participants. This was no surprise as there was a 92% indication of the absence of user training or awareness campaigns. More interesting was the contradictions in the responses; for instance, one claimed to know what hacking is, but when asked whether s/he had been a victim or not, the response was "I don't know". The statistics of knowledgeable participants is 94%, yet 24% don't know whether they were victims or not of hacking. Similar patterns were observed with other threats too. When it comes to awareness of policies in the organisation, the most popular policy was known to 29% of the participants. When it comes to configuring security, 46% have done so and 54% not; however, when asked about which

embedded security features they use in their programs, contradictorily, 61% use passwords, 20% use permissions and 15% use encryption. The question is what the 46% configured, as only 3% said they used other embedded security mechanisms.

The literature review also established the importance of awareness of all the aspects of user experience and information security, both at personal and organisational levels, as depicted in the theoretical framework.

The literature survey in Chapter 3 has established that an End User Security Feature is an embedded security function in an end user program that achieves InfoSec goals at program level. These are also security functionalities embedded within other products (EUP), as shown in Figure 6-7.

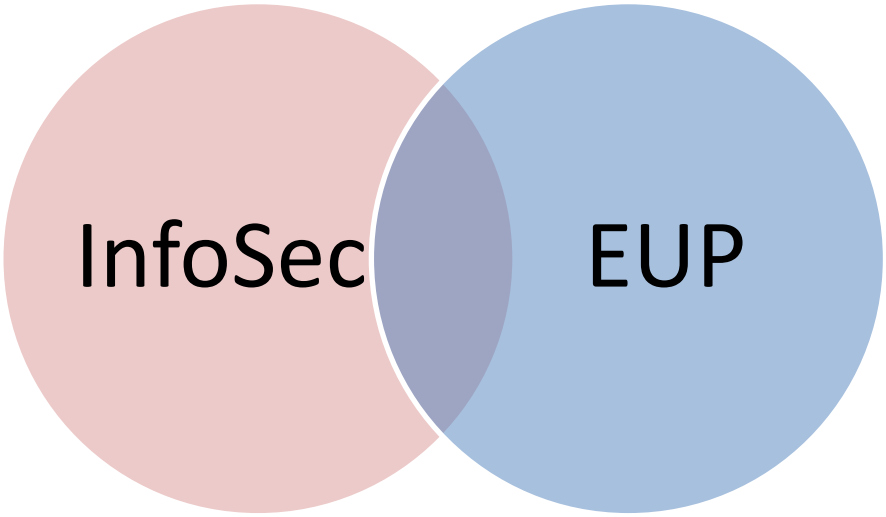


Figure 6-7: EUPSF relative to InfoSec and EUP

Factors that affect the user experience with EUPSF interaction include the fact that security features (alerts, dialogue boxes) are rarely displayed; they are too complex for end users to understand and implement. Sometimes end users are presented with options that do not lead them to making the right security choice (Whitten & Tygar, 2005; Herzog & Shahmehri, 2007). Furthermore, designers use technical jargon to describe the features (Furnell, 2006). The features

usually present unclear functionality, minimal or no feedback, forcing uninformed decisions (owing to lack of knowledge) (Furnell, 2006).

Interaction involves a product which, in this study, comprises the end user program security feature and an end user. To evaluate UX of the interaction successfully, EUPSF characteristics have to be evaluated for adhering to UCD and design for UX. Product document and literature reviews were used in the research to identify the features as outlined in Chapters 3, 4 and 5. End users reviewed EUPSF for usability and UX issues. Questionnaires and peer/expert reviews validated EUPSF. UX and USec experts employed heuristic evaluations to assess the features. The evaluation criteria were refined, based on the findings, and are presented in Appendix B1 and B2.

Chapter 4 focused on defining and characterising User Experience (UX). It exists as a result of user interaction with security in context. The context, in this case, comprises the EU characteristics, InfoSec goals, EUPSF characteristics, and the program in use which, in this study, is Adobe Acrobat Reader or MS Word, and the organisation. The organisation has a security culture, which is achieved through several security policies. User experience is at the heart of all these elements, as shown in Figure 6-8.

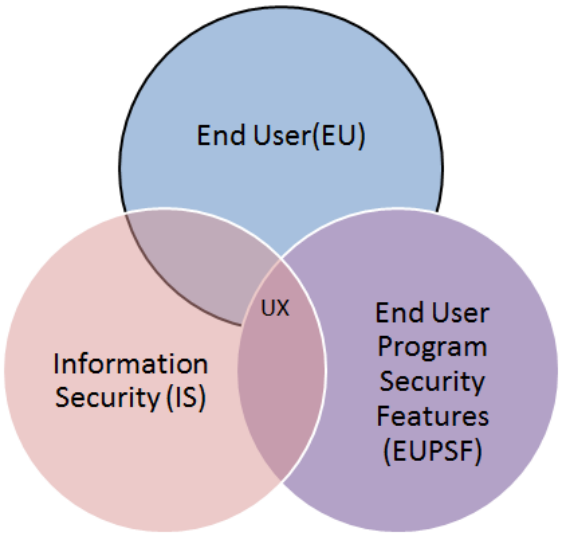


Figure 6-8: UX relative to other constructs

Questionnaires were used to survey user experience with their interactions. Experts from InfoSec and UX fields conducted heuristic evaluations of EUPSF in MS Word and Adobe Acrobat Reader.

As defined in Chapter 4, Section 4.2, it is a process which includes protecting information integrity, confidentiality and availability on end user devices and on networks. Security is not the primary responsibility for the users; hence, they do not have the commitment to learn and understand it. End users regard security as a bother/abstraction from their primary task as they are usually required to respond or interact with a number of dialogue boxes to complete a single security task. Figure 6-9 shows factors that affect InfoSec.

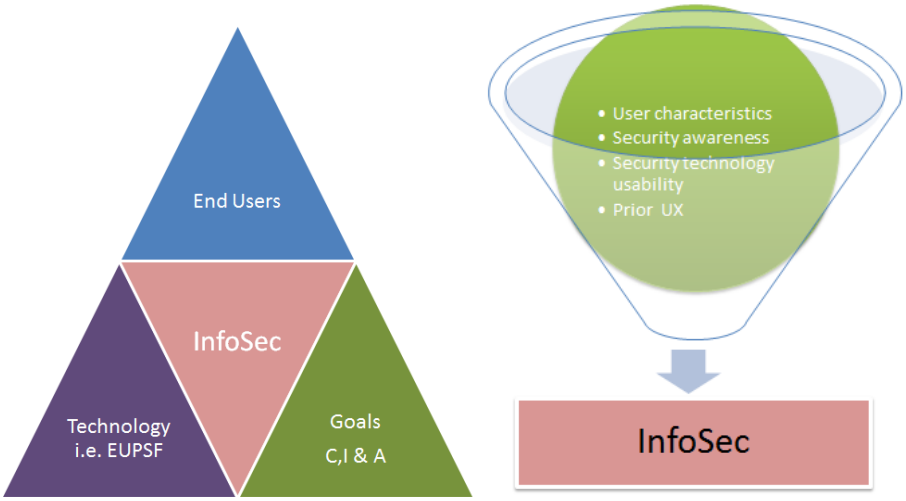


Figure 6-9: Factors affecting InfoSec

Goals speak to the individual as well as to organisational goals. Organisational goals shape the security culture in context through security policy documents, technologies and processes, which are implemented primarily to achieve confidentiality (C), integrity (I) and availability (A). From the user's perspective the security should be visible, usable, appealing and should satisfy their personal goals.

Earlier on, the research was demarcated not to focus on organisational culture; hence, to evaluate UX successfully, the focus will be on USec. User studies (empirical) have shown that end users have a negative experience with security interactions. To ascertain the extent of the problem and to influence UX, Usable Security heuristics were identified for two case programs and evaluated by peer and expert reviewers through cognitive walkthroughs. User studies are another option;

however, in the light of the fact that the end users are not trained on security, peer reviews would be more informative. Generally, the features are not easy to locate, they are not logically grouped and they require a great deal of effort to locate and apply them.

6.3.3.3 Phase 3 - Stage 3: Construct relationships

Component identification was done in phase 2. In this section the relationship between the constructs is presented. Figure 6-10 shows relationships for all constructs involved. Direct relationships between constructs are also presented in the figures following

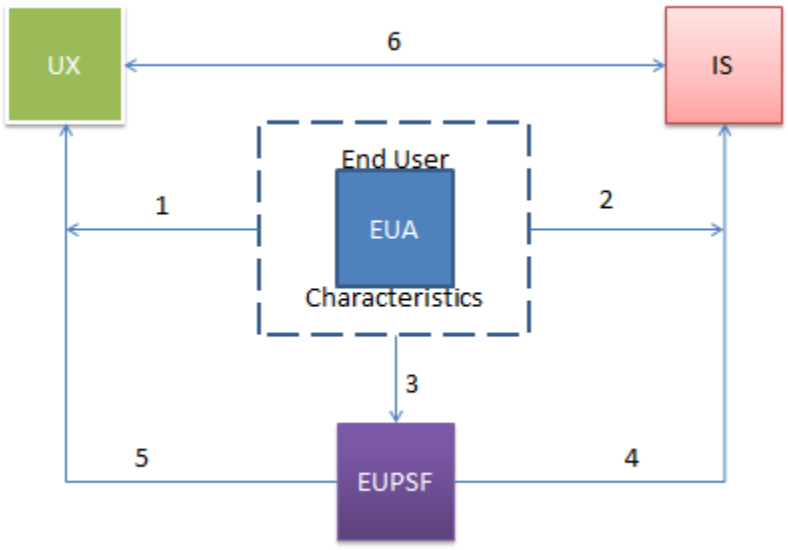


Figure 6-10: Construct interrelationships

Relationship 1 is between end user characteristics and user experience (motivation and interest missing). Figure 6-11 shows how EU and UX relate to each other.

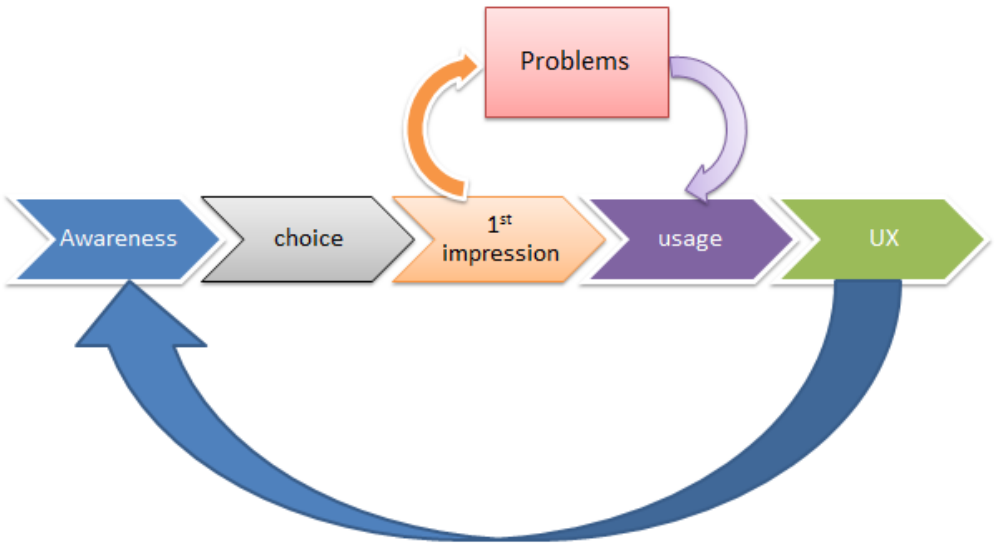


Figure 6-11: User awareness - UX relationship

Relationship 2 is between **EU** and **IS**. Users are motivated to achieve information security goals (confidentiality, integrity and availability); however, this depends on both user and security characteristics. The user, first and foremost, needs to have awareness of the existence and the need for information security. The users' experience and perception of security and their interaction will result in whether or not their information is secured. Secure interaction/usage of EUP will influence further security usage while loss of information may be a deterrent, as the user will develop resistance to use security. User characteristics influence the state of information security in most cases; the smaller part is attributed to the technology. The relationship is presented in Figure 6-12.

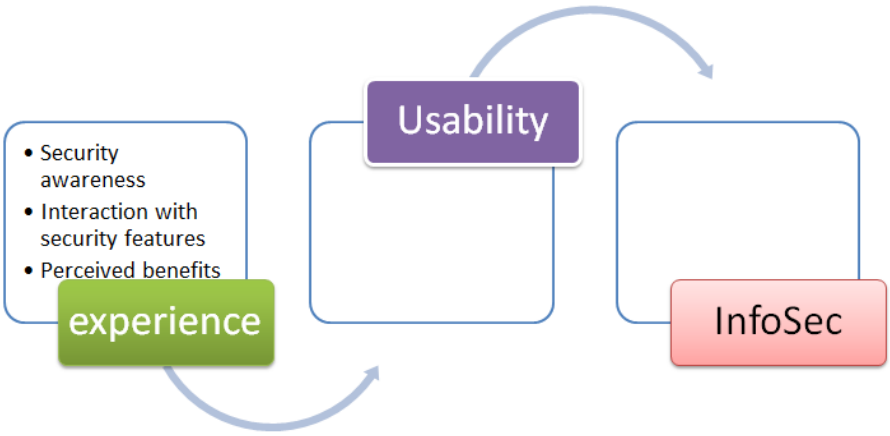


Figure 6-12: EU characteristics and IS

Relationship 3 is between EU and EUPSF. **EUPSF** has characteristics that influence user characteristics, such as behaviour, emotions and perceptions. End user characteristics, in turn, determine whether EUPSF are used as they are designed to do, or not. EUPSF are designed to achieve the EU's security goal if, and only if, the EU uses them correctly.

Relationship 4 is between EUPSF and IS. **EUPSF** are a subsect of **IS** and fulfil the goals of **IS** within an end user program**.** Organisational IS goals are achieved through cumulative security achievements in all computer system components of which end user programs are the most used and most vulnerable. Usage of EUPSF results in IS, a lack of which leads to information loss and compromises.

Relationship 5 is between EUPSF and UX. Characteristics of an end user program security feature including usability determines the user experience and the experience, in turn, creates an impression of the feature. Positive impressions result in positive attitudes towards the interaction and better information security.

Relationship 6 is between IS and UX. IS goals and usability determine UX while interacting with a program. If the security goals are in line with end user goals the user is motivated to achieve them. IS goals are achieved through usable security technologies. The better the usability; the better the satisfaction with the usage; hence, the user will remain with a positive experience and anticipation to use the technology again. UX therefore determines user

behaviour with IS and the overall IS posture. If the experience is negative, the end user is not motivated to use it and the result is compromised (low) information security. Figure 6-13 summarises the relatedness of IS to UX.

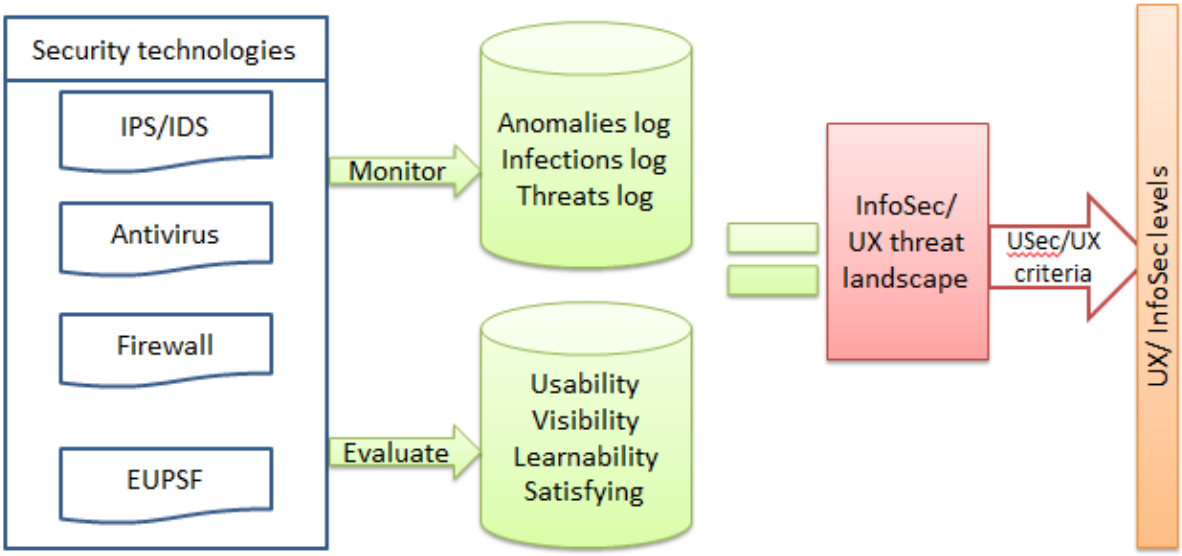


Figure 6-13: InfoSec-UX relationship

End user awareness (EUA): End users need to be aware of all the other components and their characteristics. EUA determines the usability of EUPSF, and determines UX and overall InfoSec.

Refined theoretical framework showing the framework components: The modified framework is composed only of the four components necessary for the successful evaluation of UX end user security features. User characteristics are at the centre influencing UX which, in turn, influences EUPSF usability and the overall organisational information security posture.

The first step towards developing a conceptual framework was to identify the factors that affect the security of user experience with EUPSF interaction. The identified components were connected as shown in Figure 6-14.

Figure 6-14: All components relatedness

If users are aware of security threats, security technologies and embedded security features, they interact with and use security technologies to protect themselves. Knowledge enables end users to enjoy securing program information from threats and, therefore, to maintain information security. Security awareness is at the core of information security as it determines the feeling invoked by interaction with a EUPSF. Feelings determine the attitude towards interaction and; hence, influence the user experience. Prior experience shapes user behaviour with security features. This, coupled with EUPSF usability determines the overall security posture. Since user behaviour is complex and beyond the scope of the study is deliberately excluded from the theoretical framework presented in Figure 5-6.

6.3.3.4 Phase 3 – Stage 4: Tentative design

Figure 6-15 is a conceptual design showing the links among the different components of the EUPSFUX evaluation framework. The framework can be used by InfoSec experts to evaluate the usability of the EUPSF, security awareness and the impact on general InfoSec in an organisation and to inform them of suitable interventions. UX experts can use it to evaluate how the actual UX compares to the designed UX. This will inform them on how to influence positive

experiences in the context: they can propose interventions to InfoSec experts; or the IT technical team can use it to determine focus areas for their security awareness programs in the organisation. The conceptual design shows how the UX is influenced by context which, in this case, is the organisation and their InfoSec policies, the end user characteristics - including the goal in engaging with an EUP - as well the EUPSF characteristics.

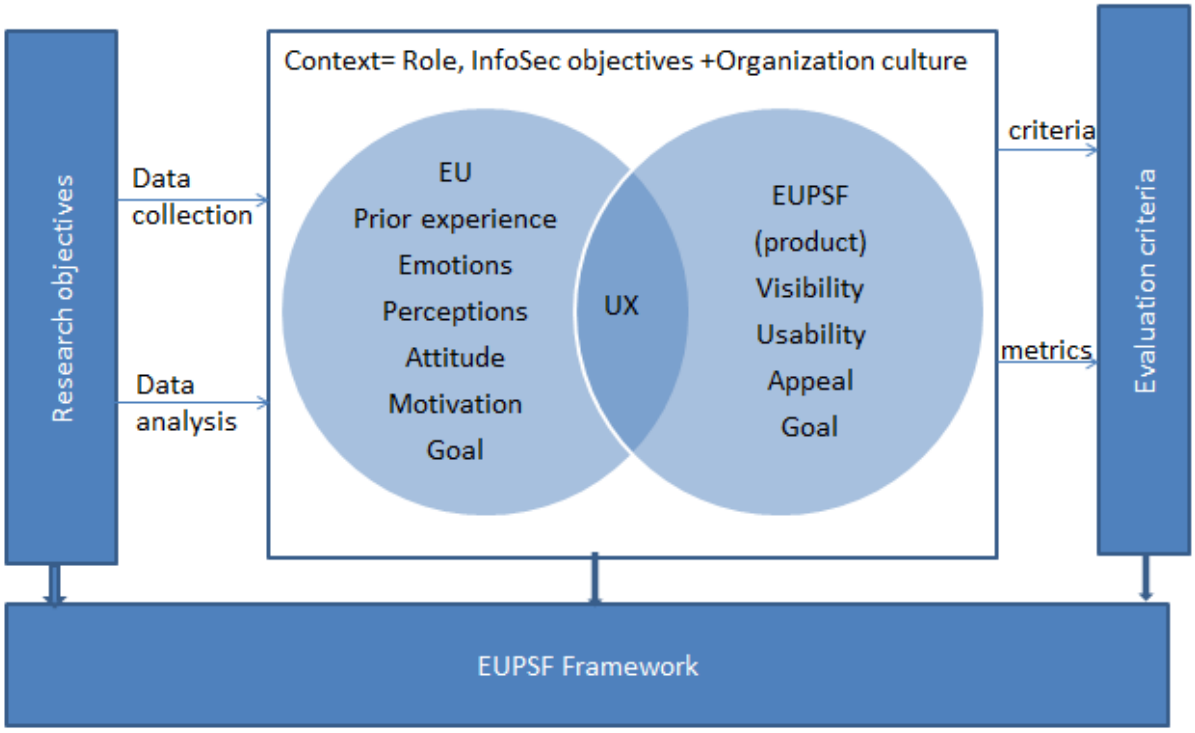


Figure 6-15: Conceptual relationship

Figure 6-15 shows how the different constructs identified in addressing the research objective are linked in designing the EUPSFUX framework. The evaluation criteria and metrics were derived from literature. Each field of study making up the components of the framework has factors that influence UX. These factors can be evaluated for their effect and influence. The combination of the different criteria formulates the criteria for the designed framework, as shown in Figure 6-16. The evaluation criteria resulting from the process depicted in Figure 6-16 will be used to evaluate different stages of the framework implementation by both InfoSec and UX practitioners.

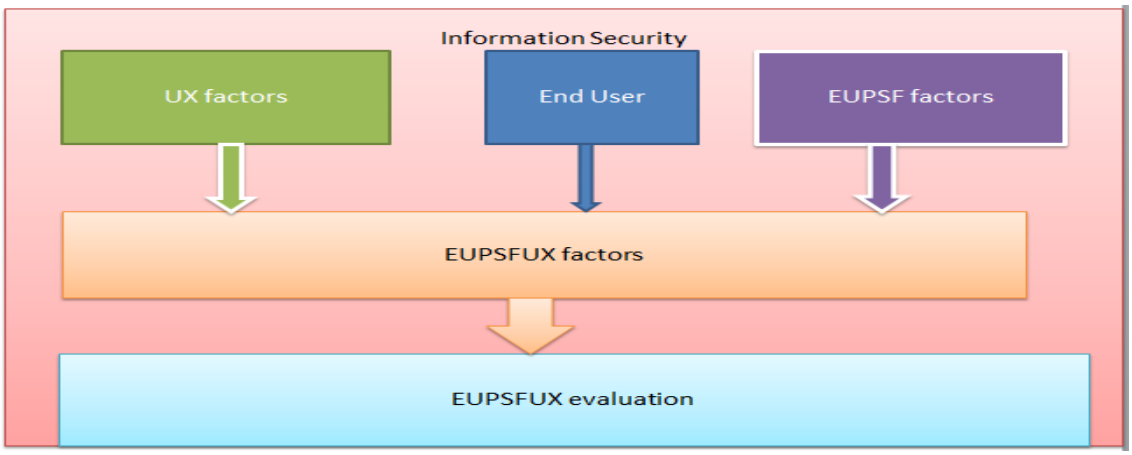


Figure 6-16: Framework evaluation derivation process

The output, in this instance, are the UX metrics, IS metrics and heuristics for evaluating the UX of the security that are presented in Section 6.7, phase 5 of the DSR process. In Section 6.1, the components of a framework were introduced as including components, relationships, evaluation criteria and implementation guidelines. The first three components have been presented. The next section discusses the implementation guidelines.

Implementation guidelines inform practitioners on how to apply the framework in a real life setup. Figure 6-17 shows the framework implementation guideline that is in five stages. The implementation stages are explained in the next section.

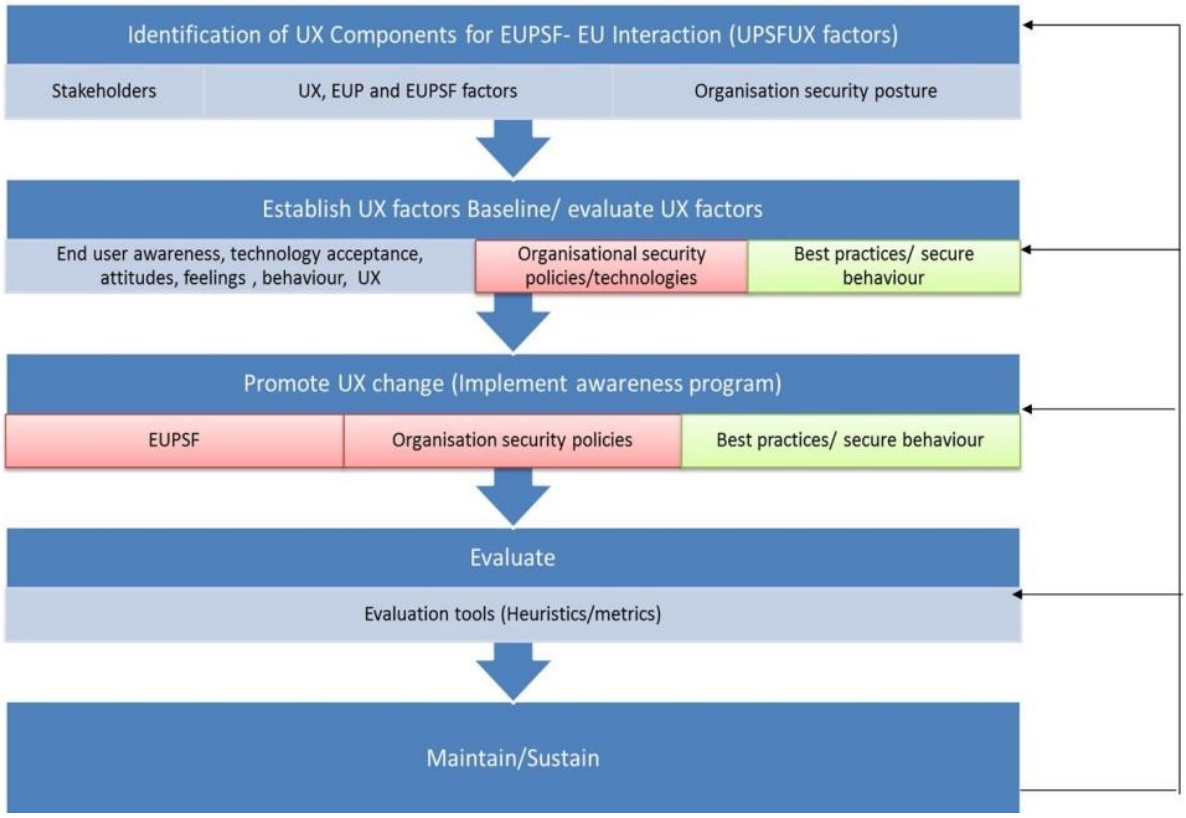


Figure 6-17: Implementation of the framework

Implementation stage 1: Identify UX factors in context. This includes three aspect of UX, namely: end users (stakeholders), product (EUP and its security features) and the context, which is the organisational security culture. These three factors were established in Chapters 3 and 4 during literature review and were confirmed in user study 1, presented in Chapter 5.

Implementation stage 2: Establish the UX baseline by evaluating the current UX state in the context. Data is collected and analysed against awareness metrics and UX heuristics. The baseline serves two purposes:

- It identifies areas that need to be improved in order to improve UX.
- It provides a reference point for assessing the effectiveness of the awareness program implementation in stage 4.

Implementation stage 3: Implement (promote UX change). In this stage intervention is implemented in the form of an awareness program that focuses on influencing factors. Findings from user studies confirm that the major influencing factor is end user awareness of security

features, threats, technologies, policies and best practices. Since UX depends on EU characteristics, it is vital to address the characteristics with the greatest impact first.

Implementation stage 4: Evaluating UX after implementing the intervention.

Implementation stage 5: Maintain and sustain. A strategy for evaluating and influencing UX periodically is put in place. This might consider upgrades or version releases. Influencing factors, such as security breaches, can be monitored against an acceptable threshold. When it gets above low level, this signals the need for intervention. To demonstrate the applicability of the implementation guideline, Table 6-4 was designed by populating each stage with possible data.

6.3.3.5 Phase 3 - Stage 5: Framework consolidation:

Now that all the components of the framework have been identified, the next stage is putting all the pieces together to achieve our objective by answering the question: "How can UX evaluation criteria and metrics necessary for end user program security features be constituted into a framework?" Figure 6-18 is a composition of all the components, according to the definition of a framework presented in Section 6.1.

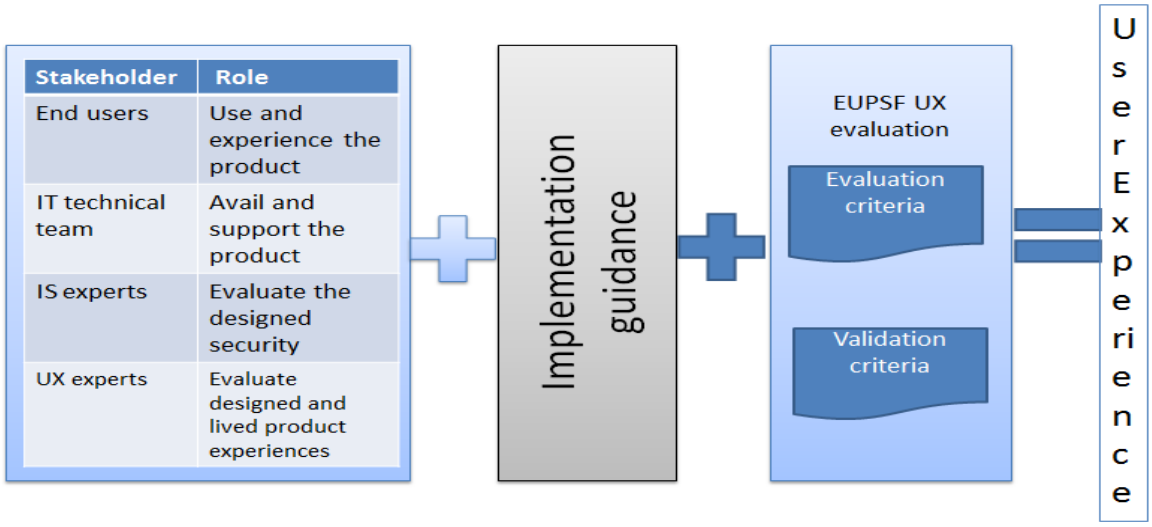


Figure 6-18: Tentative framework composition for UX experts

The proposed framework for evaluating the user experience of interacting with end user program security features is presented in Figure 6-19. The framework answers the main research question: How can a framework be designed to evaluate the user experiences (UX) of interacting with end

program security features from a user's perspective? Thus, it achieves the main research objective.

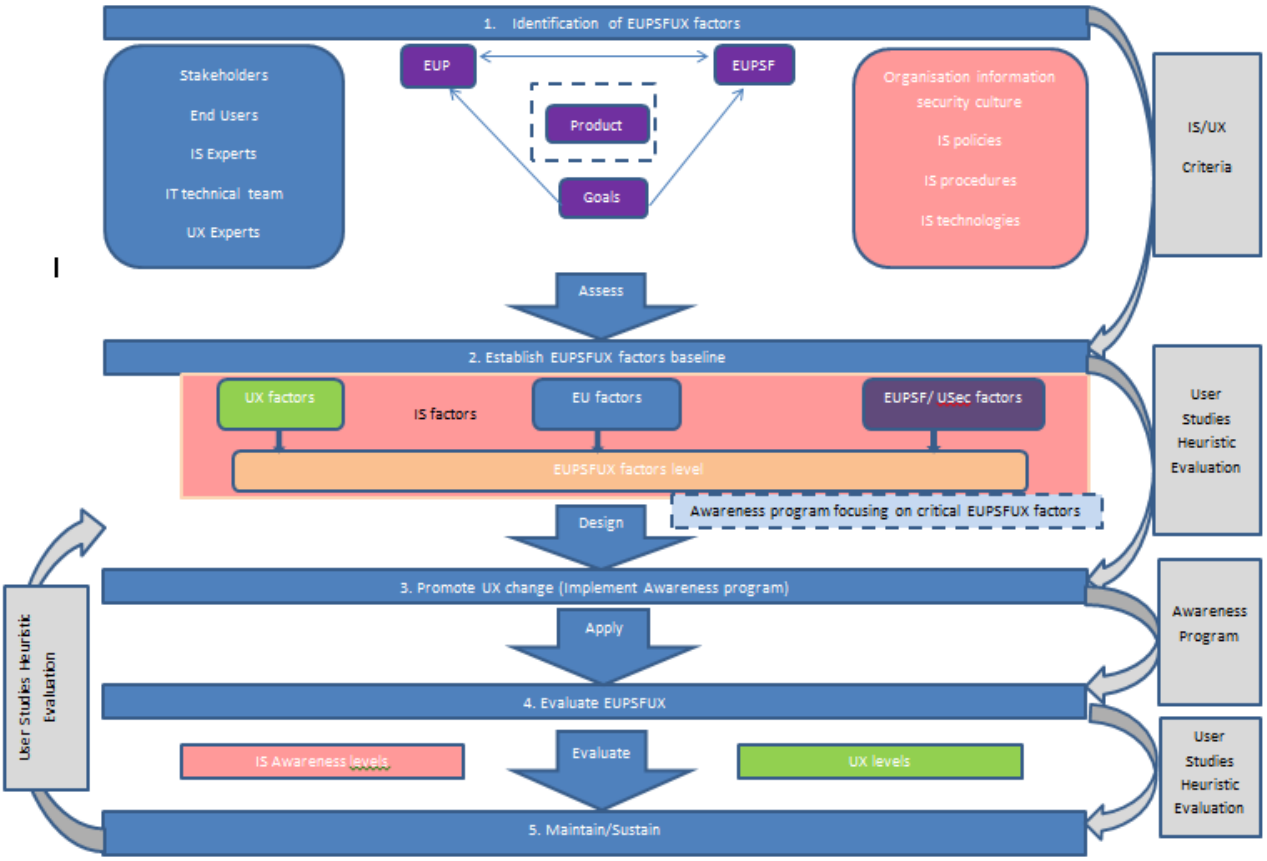


Figure 6-19: EUPSFUX framework

The components of user experience are end user program security features (products), end users, and the organisational security posture (context). They all contribute to the user experience and to the overall security posture of the organisation and have been presented in detail in Section 6.4. From the research findings the order of importance is EU characteristics especially awareness and perception which can bring change in all aspects, this should make up half of the composition, technology (EUPSF) characteristics should make up about a third of the components as it is driven by humans and influence human factors as well as the context and eventually the context shaped by organisational security culture should occupy a fifth. These components are evaluated for their characteristics and their effect on user experience through user studies, heuristic evaluations and cognitive walk- throughs. Stakeholders (UX/ InfoSec experts and IT technical team) firstly use the implementation guidelines to implement the

framework; secondly, they design, evaluate and apply UX factors evaluation criteria; thirdly, they evaluate, regulate and influence the organisational security posture; lastly, they design, choose and implement end user programs.

6.3.4 Phase 4 - Demonstration

The application of the framework is demonstrated in the following sub-sections using **theoretical validation, task scenario analysis and literature**. According to Hevner et al., (2004), artefacts created in design science research are not often implemented in practice, but they describe concepts, practices, practical competences and products innovatively, which ensures effective and efficient IS use, design, analysis and implementation. In the light of this, task scenarios will be modelled and evaluated to demonstrate the applicability of the framework. This is in line with Peffers'(2008) Phase 4 where simulations, case studies, experiments and proof of concept are used to establish the adequacy of the framework in addressing the identified problem. During the development, as well as during the evaluation of the framework, stakeholders were purposefully selected to evaluate the different stages. The following sections are part of the highlighted phase of the DSRM for the EUSFUX framework in Figure 6-20.

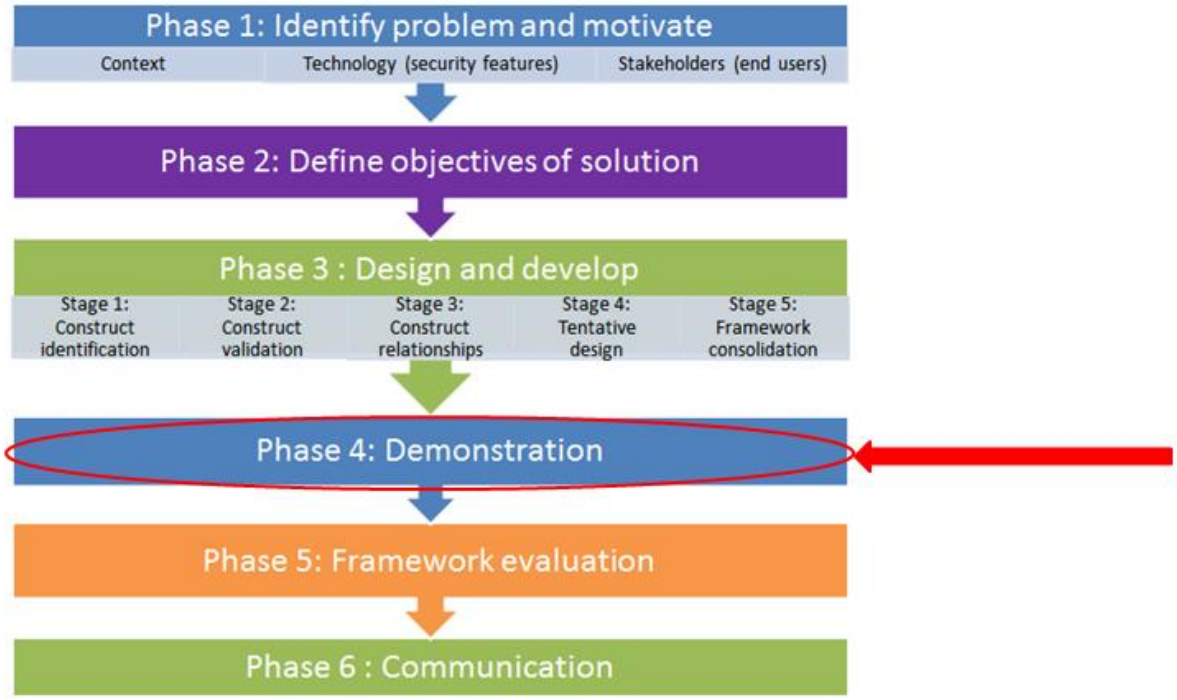


Figure 6-20: Phase 4 of the EUPSFUX methodological approach

6.3.4.1 Theoretical demonstration

Literature was used to ensure the internal validity of the proposed framework by deriving and validating the appropriateness of the proposed components. The objective is to demonstrate the appropriateness of activities and appropriateness in the UPSFUX framework in evaluating successfully the UX of EUPSF interaction as well as its utility.

6.3.4.2 Task Scenario analysis

Task scenario analysis aims to address the question: How can the proposed framework be evaluated for the successful and adequate evaluation UX of end user program security features? This is demonstrated by applying the framework on end user program security features.

Scenario-based design is a set of related user-centred techniques in which the use of a future system is explained elaborately earlier in the development process. Narrative explanations of anticipated usage incidents are used variably to direct the development of the system that will facilitate use experiences. Scenario-based design is not a formal or task- specific method; rather, it is an informal method for visualising future use options (Rosson & Carroll, 2002). The scenario details the order of actions and events leading to a result. These actions and events are related in a use context that comprises the goals, plans, and reactions of participants (Rosson & Carroll, 2002).

"A **scenario** is a **scene** that illustrates some interaction with a proposed system. A **scenario** is a tool used during requirements analysis to describe a specific use of a proposed system. Scenarios capture the system, as viewed from the outside, e.g., by a user, using specific examples." (Arms, nd)

Steps:

1. Who are the users/ actors?
2. Goal
3. Use case (a summary of scenarios for a single task or goal)
4. Use case scenarios (A scenario is an example of what happens when someone interacts with the system.)

Scenario 1: InfoSec expert:

A system administrator at the Polytechnic of Namibia was consulted about the security concerns in his organisation. The IT department is well staffed with skilled personnel; they have developed up-to-standard policies, which are comparable to those in other similar institutions; they have a call centre open from 0700 until 2200. The organisation has invested in state of the art current security technology and IT infrastructure; however, computer infections are rife and the users do not behave as expected. Table 6-4 is a demonstration of the framework implementation guide.

Table 6-4: Framework implementation demonstration

Implementation stage	Component	Attributes	Example
Identification of EUPSFUX factors	Context Organisational security culture factor	Policies	Perform a systems security audit. (Are the relevant policies in place? Is the right infrastructure properly installed and managed? What are the security risks associated with the installed technologies? What are the security technologies installed? What security processes exist in the organisation?)
		Infrastructure	
		Information security technologies	
		Processes	
	Product	End user programs	What programs are installed? Are they up to date and licenced? Audit
		Program security	What are the risks associated with the installed programs? (Document review). What are the security features in the programs? (Document review and cognitive walkthrough). Program design security evaluation against standards.
		Program goal	What is the primary goal of the program? (Program documentation)
	User	Role	What are the skills and competencies of the end user?
		Goal	What is their goal in using technology? (End user program)
Establish EUPSFUX factors baseline	UX factors	User studies, UX heuristic evaluation	Are the EUPSF appealing, beautiful, attractive, motivating, desirable, exciting or comfortable? What are user attitudes towards EUPSF interaction? What feelings are evoked by user- EUPSF interactions?

Implementation stage	Component	Attributes	Example
	User characteristics	User studies	What are the goals of users when they interact with the program? Are they motivated to use the EUPSF? Are they aware of the existence of EUPSF? Are they aware of the benefits of using them? How do they behave with EUPSF?
	EUPSF (Product)	User studies, usability and security heuristic evaluation	Are the EUPSF easy to use, easy to locate, understandable, useful, learnable, satisfactory, and effective? Do they offer assistance? Are they efficient, secure or valuable?
Promote UX change	Develop UX change strategy	Use usable EUP Communicate policies Develop and implement awareness program Influence organisation InfoSec culture	Evaluate, choose and implement EUP with usable EUPSF Promote policy awareness Promote security awareness Promote a secure organisational culture
Evaluate EUPSF factors	User	User study	Use baseline criteria to allow for comparisons
	Product	EUP review	
	Context	InfoSec culture	
	UX	User study	

Further points to consider include an understanding of the stakeholders (HR, IT department, Users, Management). Establish a baseline- review of the antivirus and system logs; conduct an awareness survey; observe or survey or log user behaviour or phishing attacks. Enumerate the severity of the problems.

Scenario 2: IT technical support team

The scenarios presented can be applicable, with a focus on the implementation of controls and usable programs.

Scenario 3: UX expert

Post-use studies were conducted at PoN and the results reflected negative attitudes towards security interaction. The users have a negative attitude towards security and they feel disturbed and frustrated by the interaction

6.3.5 Phase 5- Framework evaluation

This section describes the evaluation and validates the proposed framework for rigour and relevance in line with Phase 5 of the EUPSFUX methodological approach highlighted in Figure 6-21. The artefact evaluation findings can be presented in the form of immediate, intermediate and long-term impact, according to (Shrestha, Cater-Steel, & Toleman, 2014). This will be achieved by demonstrating quality, transferability, credibility, confirmability, dependability and utility. The EUPSFUX framework is assessed using implicit criteria that were explicitly presented in Section 2.4.6.1 and in the proposal (output of the awareness of problem phase). Table 2-5 presents the criteria and methods applicable to the EUPSFUX evaluation framework.

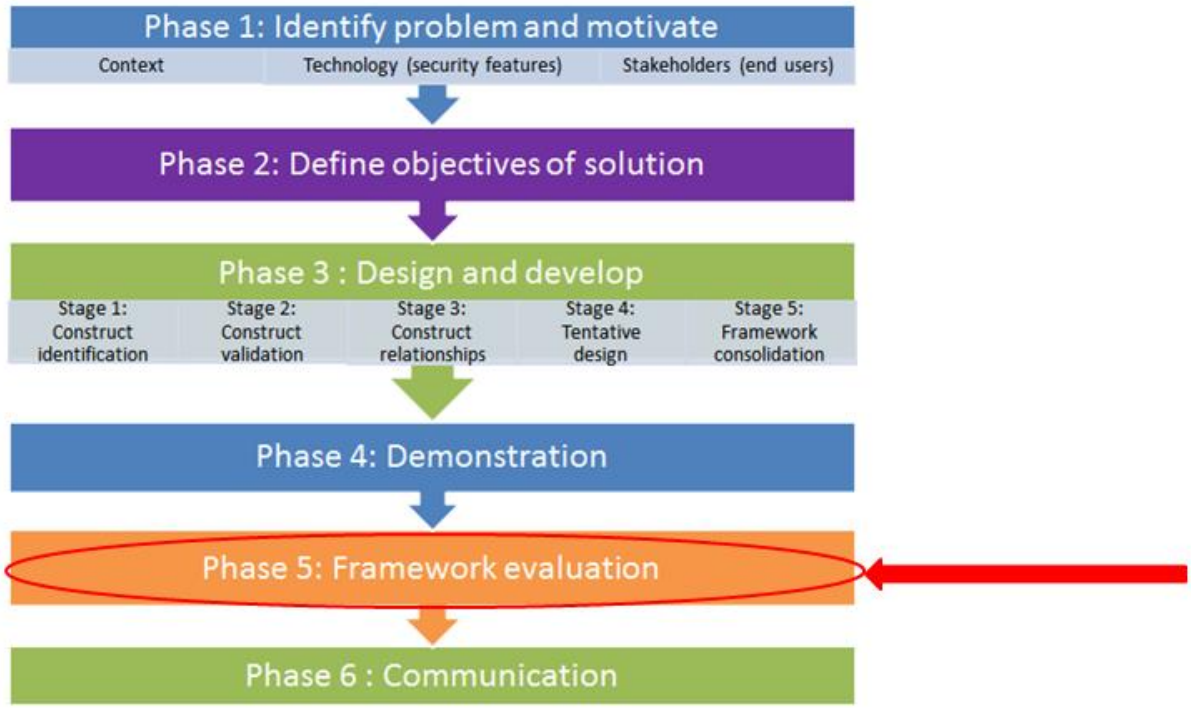


Figure 6-21: Phase 5 of the EUPSFUX methodological approach

For this study, **relevance** was established through **completeness**, and **consistency;** and **rigour** will be demonstrated through well-tested processes and methods. **Theoretical validation,**

heuristic evaluation, expert reviews and informed argumentation approaches are used to validate and demonstrate the applicability of the framework. These methods are discussed in the following sections. Completeness and utility demonstrate whether the framework meets the research goal namely "to identify USec UX metrics applicable to EUPSF". The evaluation process followed the outline in Figure 6-22.

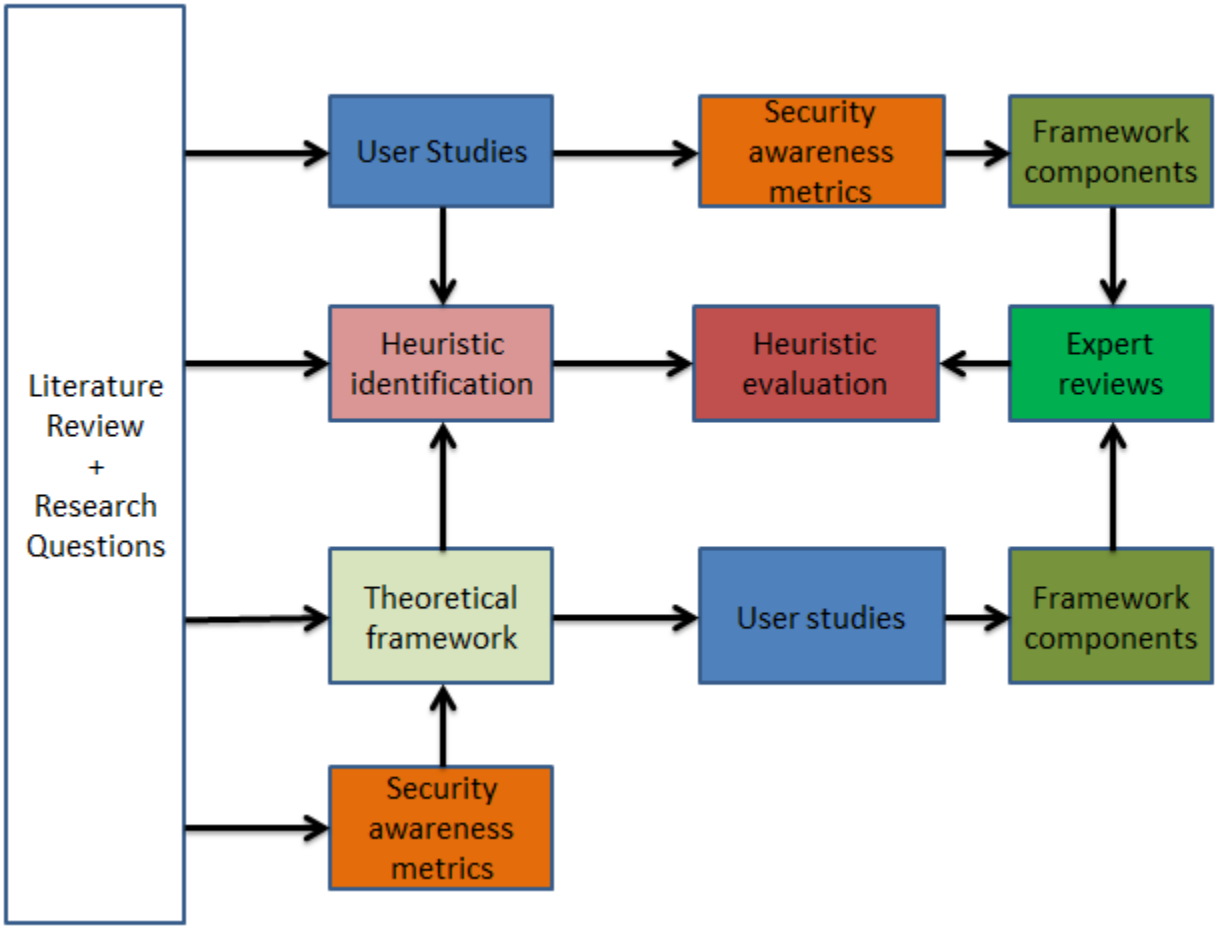


Figure 6-22: Evaluation process

The findings from the evaluation process are discussed in Chapter 7.

6.3.6 Phase 6- Communication

After iteration of design and evaluation, a final product is presented. This will be detailed in Chapter 7, which is the finalisation of the framework design process. The communication is Phase 6 of the EUPSFUX methodological process highlighted in Figure 6-23.

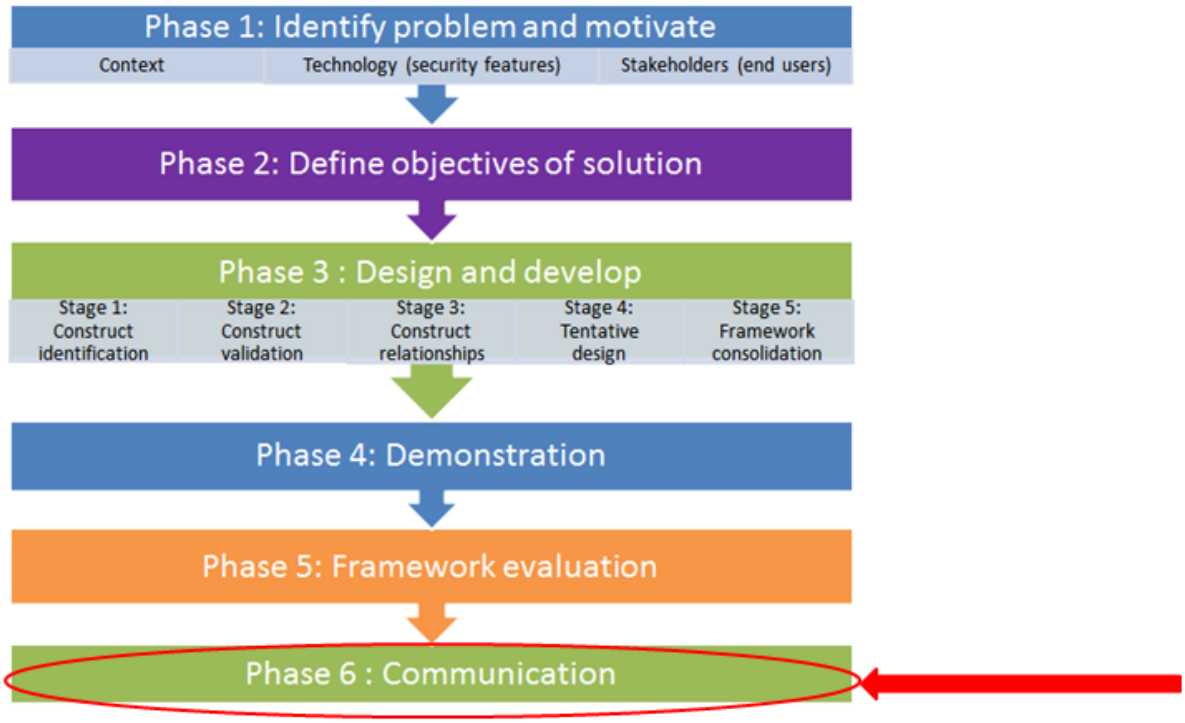


Figure 6-23: Phase 6 of the EUPSFUX methodological process

6.4 SUMMARY

Chapter 6 has described the process used to design the EUPSFUX framework. A discussion of the process and applicability for framework development is also included. The chapter discussed in detail the various components of the framework and how they were derived from the related disciplines, namely user experience and information security. Construct and construct component identification through literature review presented in Chapters 3 and 4 and the UX factors survey in Chapter 5 was also presented. The identified framework components EU, UX, EUPSF and IS context characteristics, the relationships, evaluation criteria, implementation criteria are composed into the EUPSFUX framework, as shown in Section 6.3.5.5.

The EUPSFUX framework emphasises the following aspects:

1. Identifying and understanding the factors that affect user experience, the context as well as the stakeholders.
2. Establishing the baseline of UX through surveying the UX factors and evaluating them against UX, IS and USec criteria.
3. Promoting UX change by implementing awareness programs that focus on EUPSF, organisational security policies and culture, security best practice and secure behaviour.

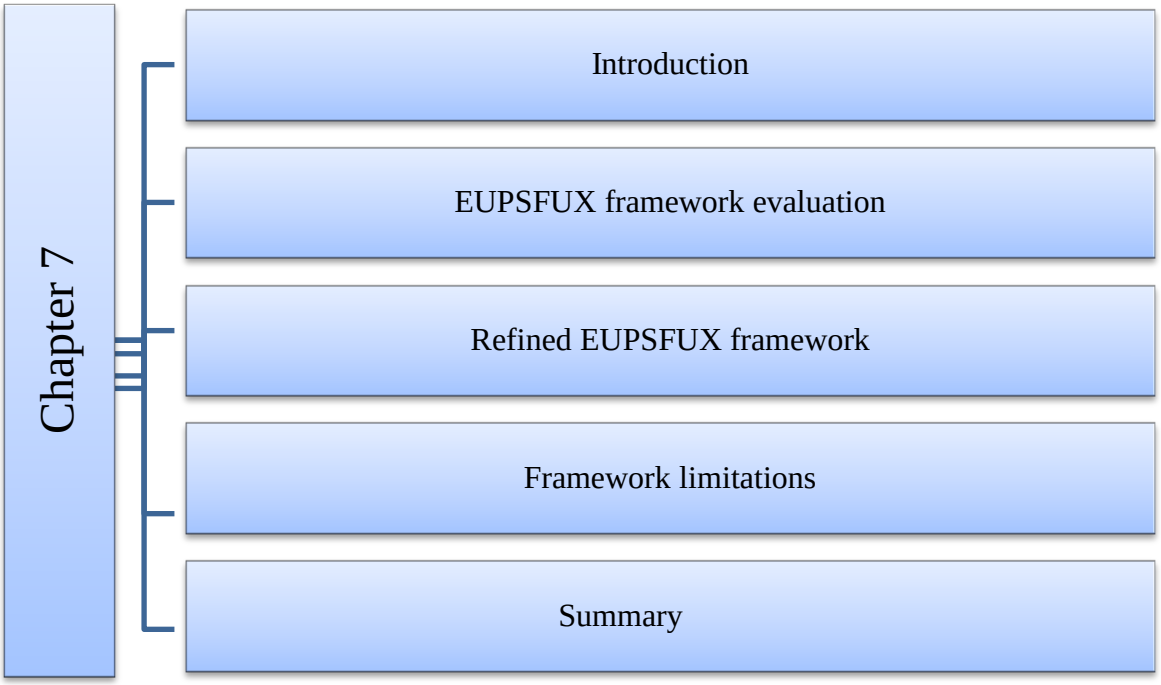
4. Measuring the impact of the awareness program on user experience by comparing it to the established baseline.
5. Maintaining and sustaining the user experience by monitoring and evaluating the awareness program on a regular basis, followed by user experience evaluation. Device strategies to continuously improve positive user experiences with program security feature interactions.

The study stakeholders were identified as end user, IT technical team, IS and UX experts. Next, the evaluation and validation of the proposed framework will be presented in Chapter 7 and the outcomes will further refine the framework.

CHAPTER 7: FRAMEWORK FINALISATION

7.1 INTRODUCTION

In line with Phases 5 and 6 of the framework development process, this chapter presents the EUPSFUX framework evaluation, the refined EUPSFUX framework, the EUPSFUX framework limitations and finally the chapter summary will be presented following the flow in chapter outline.



7.2 EUPSFUX FRAMEWORK EVALUATION

Section 7.2.2 discusses validity and objectivity of the framework to establish the quality of framework evaluation; Section 7.2.4 discusses the reliability aspect while Section 7.2.4 focuses on the relevance and Sections 7.2.5 through 7.2.7 discusses the theoretical validation through expert validation.

7.2.1 Evaluation tools

The framework was evaluated by appraising the designed components: security awareness metrics; security and UX heuristics for the artefact. The resulting framework itself was evaluated using literature and expert reviews; the implementation guide was subjected to use case scenario analysis, as demonstrated in Section 6.3.4.2. Table 7-1 is a list of evaluation tools applicable to the EUPSFUX framework developed in this study.

Table 7-1: EUPSFUX framework evaluation tools

Dimension	Method	Objective/ Target
Goal	Informed argumentation, Use case scenario analysis, expert reviews	Efficacy, validity
Environment		Fit with organisation (relevance)
Consistency with people	Use case scenario analysis	Ease of use
Consistency with technology	None	None
Consistency with organisation	Use case scenario analysis	Utility
Structure	Informed argumentation	Consistency
	Use case scenario analysis	Completeness
Activity	Informed argumentation	Consistency
	Informed argumentation	Completeness (functionality)
Evolution	Use case scenario analysis	Learning capability

7.2.2 Quality of the EUPSFUX framework

Care was taken, throughout the design phase, to ensure that it demonstrates construct validity, internal validity, external validity, objectivity and reliability. Construct validity requires the researcher to use the correct measures for the concepts being studied. Internal validity demonstrates that certain conditions lead to other conditions and requires the use of multiple pieces of evidence from multiple sources to uncover convergent lines of inquiry. External validity reflects whether or not findings are generalizable beyond the immediate case; the more variations in places, people, and procedures that a case study can withstand and still yield the same findings; the more there is external validity. Techniques such as cross-case examination and within-case examination, along with literature review, help to ensure external validity. Objectivity is the degree of independence from researcher bias. Reliability refers to the stability,

accuracy, and precision of measurement. The procedures used are well documented and can be repeated with the same results over and over again. (Yin, 2009; Dooley, 2002; Oates, 2012).

7.2.2.1 Validity

The research paradigm followed in this research is interpretivism; hence, reference is made on how much trust can be placed in the research instead of validity. Trustworthiness is the level of trust that can be placed in the research based on the use of valid methods and techniques derived from literature to measure framework components.

External Validity/ Transferability is the extent to which the research is generalisable to different environments, participants, and time; and it depends on the representativeness of the sample studied (Oates, 2012, p. 294). However, environmental aspects such organisational culture, and personal dispositions make it impossible to apply the same process in a different context. Instead, focus is put on transferability of the findings to other, similar contexts.

Transferability is demonstrated through documentation of the tools and methods which were used in designing and validating the EUPSF.

Internal/Credibility validity is the degree to which findings are precise, compare to reality and measure it correctly; however, in interpretivist research there are several created realities; hence, there is no benchmark for testing the results (Oates, 2012, p. 294). Instead, the focus is on credibility of the research process. Triangulation of methods (interviews, surveys, peer and expert reviews, and heuristic evaluation), strategies (case study, surveys and design and creation) and data (literature, interview, survey, heuristic evaluation, peer and expert reviews) are used to demonstrate this aspect. The findings reflect the programs have no means of educating the user on the existence and use of embedded security functionalies and their benefit.

7.2.2.2 Objectivity/ Confirmability

Objectivity cannot be demonstrated in this case because the researcher has personal experiences that can influence the interpretation of collected data. Moreover, the researcher is a member of the community being studied and interacts with participants often. As such, focus is placed on the demonstrated confirmability of the findings. Given the collected data, summaries and the analysis, another researcher can draw the same conclusions.

To demonstrate confirmability, the following tools and methods were used:

1. Clearly outlined methods and processes were used for data collection and analysis
2. Use of literature to confirm findings

7.2.3 Reliability/Dependability

Reliability is usually centred on repeatability of the study; however, when a social problem is studied, it is bound to vary at different times as the influencing conditions evolve. As such, data collected at different times cannot be similar (Oates, 2012, p. 294; Hevner et al., 2004). Moreover, as the researcher's involvement impacts on the outcome, different researchers will produce different results. It is best to demonstrate the dependability instead, as it speaks to the research procedure and data recording, which allow an audit to be carried out successfully on the research process (Oates, 2012, p. 294).

To demonstrate dependability, the following tools and methods were used:

1. The survey was self-administered to eliminate bias.
2. Research methods and strategies are clearly documented in Chapters 2, 5 and 6.

7.2.4 Relevance

Relevance of the EUPSFUX evaluation framework is demonstrated in Section 6.3.4.

7.2.5 Theoretical validation

Theoretical validation was conducted using peer and expert (heuristic) reviews, as well as informed argumentation (against standards and theories) in a case study setup

7.2.6 Heuristic evaluations

EUPSF were validated through task-oriented heuristic evaluations by peers and experts in the HCI, InfoSec, USec and UX fields in two different case programs. The heuristic evaluation item had checklists of security tasks specific to case programs (Word and PDF reader), which were evaluated during execution. Heuristic evaluation is a fast and cheap method used to check interface compliance with recognised heuristics (Nielsen , 1995). The process involves eight stages: planning, selecting evaluators, selecting the program to evaluate, determining a set of heuristics to evaluate, prepare to collect data, developing tasks for evaluators, conducting the evaluation and finally, analysing the data. The process followed a multiple case study strategy, as

it allows for comparisons and increases the generalisability of findings by enhancing external validity. The six steps of case study research were followed in line with the eight heuristic evaluation stages. The next sections will present the process followed, step-by-step.

7.2.6.1 Planning

Multiple case programs are used to evaluate the USec UX metrics (heuristics) in end user programs. The participants, in this case, are mainly practitioners in the domains of study and they comprise of peers and experts. According to Danino (2001), planing usually involves one of the following three approaches:

1. Develop a set of tasks and ask evaluators to carry them out.
2. Provide evaluators with the goals of the system, and allow them to develop their own tasks.
3. Ask evaluators to assess your dialogue elements

In this study, the first option was employed whereby EUPSF specific tasks were given to the peers and experts to evaluate using HE.

7.2.6.2 Evaluator selection

According to Patton (1990), intensity sampling is used in heuristic research as it permits the researcher to benefit from the rich personal experiences of the participants. This was combined with stratified purposeful sampling as representatives were chosen from different fields (InfoSec, HCI, UX and USec) pertaining to the study, as well as representative of different stakeholders identified for this study. The peers represent IT administrative support, both in the case organisation and outside, as well as typical end users in the organisation as they are students at PoN. Literature on usability evaluation stipulates that a maximum of four experts is sufficient for comparison, while for user studies two end users are acceptable (Nielsen, 1994; Usabilityhome.com). Literature has it that 3 to 5 experts can unveil 75% + usability issues, while novices will uncover 22 to 29% issues (Nielsen, 1995; Balatbat, 2013). According to Danino (2001), if more evaluators are used, then more usability problems will be revealed; however, he attests that the cost/benefit ratio decreases at about five evaluators. This research is multi-disciplinary, so to capture the different disciplines in depth, 16 evaluators were selected. Peers

are not as experienced in their domains; hence, to some extent they gave end user views. Table 7-5 is a summary of expert and peer reviewer profiles.

7.2.6.3 Design – Selecting the program

The heuristic evaluation tools and associated tasks for the two EUPs were developed using a combination of tested heuristic evaluation tools by considering the specific security features and tasks for each, as well as findings from user studies. The case program selection is presented next.

Case program selection criteria

Case programs were selected based on the following criteria:

1) Program popularity in the case site and globally

2) Development following user-centred design principles

3) Integration of security in the design process

4) UX goals in the design process

5) Availability of security features in the programs

6) Prior work on usability and UX evaluation

Program popularity in the research case study and globally

A survey conducted showed the most frequently used end user application programs (EUP) in the case site and, naturally, these were the choice for the study. The applications matched with what other researchers had already identified in other studies (Furnell, 2010; SANS, 2011). The most popular end user programs were email clients with 100% uasge rate. The second most popular programs in this case were web browsers, as confirmed by 92% usage. This compares very well with literature. Web browsers are popular end programs owing to the shift to online business, socialising and education in the technology era. According to W3Schools (n.d.), the most popular browsers are Google Chrome, Mozilla Firefox and Internet Explorer (IE). After almost four years on the market, Google Chrome took over from Mozilla Firefox from 2012; Mozilla Firefox had been an equal competitor to the old-time leader, Internet Explorer in 2008

and since 2009 it had taken a lead over IE. The same web browsers are used in the case organisation as confirmed by the survey findings.

Since users use a diversity of devices with a diversity of platforms to access the web, pdf has become the indispensable tools for cross platform compatibility. Adobe Reader has become a popular tool for enhancing transferability of electronic documents making it one of the most popular programs used today. In most organisations the most popular end user programs include Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office (Bhunu, Shava & van Greunen, 2013; SANS, 2011; Furnell, et al., 2005).

Considering the diversity of web browsers on the market and different approaches to security, the researchers chose to shelve them for a dedicated comprehensive study. The focus was then streamlined to MS Word and Adobe Acrobat Reader, as they satisfied the criteria presented earlier. The compliance is demonstrated in Table 7-2.

Table 7-2: EUP compliance to selection criteria

Criteria	**Compliance**
Program popularity in the case site and globally	MSWord has a popularity of 86 in the site, globally 92% (Furnell et al., 2005; SANS, 2009; SANS, 2011) Adobe and MS Word
Development following user-centred design principles	Program documentation of both articulate to this
Integration of security in the design process	Program documentation of both articulate to this
UX goals in the design process	Program documentation of both articulate to this
Availability of security features in the programs	Program documentation of both articulate to this, as well as program interfaces, tools and menus.
Prior work on usability and UX evaluation	Furnell, 2005; Furnell, 2006; Furmell, 2010 ; Furnell et al., 2005; Schulze & Kromker, 2010; Nielsen, 1994

7.2.6.4 Determining a set of Heuristics to evaluate

The process followed identifying the security features in selected programs through document reviews and cognitive walkthroughs. In this section, Adobe and MS Word specific features are presented.

User experience in end user programs is incorporated through features. In Office 2013 the following features have improved the user experience (Microsoft, 2013):

1. The Trust Center and message bar, trusted locations, trusted publishers, and sticky trust decisions
2. Actionable security prompts
3. Improvements to the Encrypt with Password feature
4. Document Inspector
5. XML file format support

Through program document reviews for Adobe Reader and Microsoft Office, a number of elements were identified for these most commonly used programs in general, and in particular, to the case studied. These are presented in Table 7-3 (Microsoft, 2013; Adobe, 2012).

Table 7-3: Security features in Adobe and MS Office

Elements	MS Office	Adobe
Protected mode	+	+
Tighter integration with built-in, always-on		+
PDF Whitelist		+
Secure product lifecycle		+
Auto update	+	+
Patch management	+	+
Active content (active X controls, add-ins, data connections, macros, spreadsheet links)	+	
Enhanced security/Turn on or off your security and privacy features		+
Alerts	+	+
Dialogue boxes	+	+
Security agents	+	
Office assistant	+	
Permissions	+	
Document flow protection	+	
Cryptographic agility	+	
Office file validation	+	
Expanded file block settings	+	
Integrity checking of encrypted files	+	
Data Execution Prevention (DEP) support;	+	
Group policy enforcement,	+	
Trusted time-stamping support for digital signatures,	+	
Domain-based password complexity checking	+	
Enforcement and encryption	+	
File block	+	

The characteristics presented in Table 3-4 can be used as the criteria to measure how usable a security feature in a program is.

Heuristics development: The Usable Security and UX Heuristic Evaluation tool design

In Chapter 1, the research was delineated to focus on USec evaluation based on the understanding that end user program security features are designed for usability by following UCD principles. To evaluate compliance of security features to usability principles, the heuristic evaluation tool was developed following the three-stage heuristic process for specific application domains by van Greunen, Yeratziotis, and Pottas (2011). The heuristics were based on Yeratziotis, Pottas, and van Greunen's (2012)'s usable security heuristics for online health social networks; Nielsen's (1994) heuristic evaluation tool, as well as the computer system usability questionnaire and practical heuristics for usability evaluation. The heuristics are also based on usability criteria as applicable to security features identified in Section 3.6 For each heuristic, a list of checklist items is provided. Checklist items are criteria for measuring the heuristic in question. The tool has as an extent field for each checklist, which can have a value between 1 and 5. 1 is very difficult, 2 is difficult, 3 is moderate, 4 is easy, and 5 is very easy. The extent can be used to calculate each metric score per EUP and to determine the criticality of usability in determining the focus area for intervention.

The validation tool was designed in MS Word and comprised the purpose, expert profile (qualification and specialisation), list of tasks, instructions, heuristics and associated checklist items assessment. In total, 16 high level heuristics for security and UX were identified for the two programs.

The heuristic developed and associated checklists are presented in Appendix B1 for Adobe Acrobat Reader and in Appendix B2 for MS Word. The purpose of the evaluation is to determine the awareness plus usability and UX of the embedded security features in two case end user programs (MS Word and Acrobat Adobe Reader). The outcome will inform what the user awareness program in the case site should focus on and will inform the metric (heuristic) for UX in the case site. However, on a general note, it should inform security and security UX designers on how to improve the features for better usability and UX.

7.2.6.5 Prepare to collect data

Prior to collecting the data, a cover letter was designed and the heuristic evaluation tool was pretested. The next sections will talk to this.

Cover email

A cover email was designed explaining the purpose of the study as well as establishing rules for confidentiality and ethical conduct. The cover email was sent to the peers and experts along with the two tools. The email is provided in Appendix A3.

Heuristic pretesting

The tools were sent to three experts in InfoSec and USec for pretesting. The feedback did not come for three months and the tools were deployed in their original format. One of the experts later responded and made the comments in Table 7-4. The comments were used to polish the tool for future use.

Table 7-4: Improvements on the HE

Section	Item	Comment	Action
Demographics	Research area	Are you providing a separate key for the abbreviations?	No need as it is designed for field experts
Procedure	Instruction specified seven tasks in the Adobe HE tool	Nine tasks	Corrected
Note	Extent scale	From using games, etc., usually 1 is easy and 5 very difficult	Was based on existing psychology evaluation criteria as a way of ensuring that values are not inserted without thought, especially with the peers. Standard heuristic tools apply the scales similarly (bad to very good, unlikely to likely)
Typos	Missing word 1.3 17.12, 18.1	Insert feature at the end Delete the word “the”	Corrected Corrected

7.2.6.6 Developing tasks for evaluators

The tasks were developed through cognitive walkthrough and following the EUP security help documentation. Two sets of tasks were developed; one for each program. There were seven (7)

tasks for MS Word and nine (9) for Adobe Acrobat Reader. The tasks are incorporated in the respective heuristic evaluation tools in Appendix B1 and Appendix B2.

7.2.6.7 Heuristic evaluation

Sixteen domain experts and peers were individually presented with a set of security tasks to perform in MS Word and Adobe and to comment on overall security and UX of the interaction. The expert and peer review aimed at evaluating the relevance of the proposed heuristics. It also served the purpose of evaluating how the potential users of the model found the proposed model to be useful and applicable to managing user experience. The expert reviews were conducted through a heuristic tool, which was emailed to subject domain experts and peers for completion.

Some of the evaluators chose to evaluate one case program instead of both. The participants represented the technical stakeholder, who is usually tasked to design, evaluate and implement security in typical organisations, as well as the end user in the case site. Eight experienced InfoSec, UX, USec and HCI experts ,who are aware of security challenges in the case and four of whom have been associated with the case site for around five years were selected (Shneiderman & Plaisant, 2005).Expert reviews were carried out with three doctoral students, four doctors and one professor, who are practising in the target fields. Peer reviews were carried out by eight system administrators, who are studying towards their honours and Masters qualifications in the studied organisation. As was established in the empirical study, PDF viewers and Word processors are the most popular software. As such, the evaluations were conducted on these two end user programs.

The experts and peers completed a list of checklist tasks and indicated their responses, the extent to which they believed in their choices and they optionally commented on the checklist items. Comments and responses from experts and peers in the fields were used to validate the suitability of the heuristics. End users were not used for security feature usability and UX evaluation because, during the empirical study it was noted that the users are not trained on security and, as such, a user test on usability and UX would present complexities for them. Hence, the collected data would reflect the issues as much as would experts.

The expert reviewers critique program security features to determine conformance with a list of usability and UX heuristics by using the program to complete usual security tasks. UX was

measured from a usability as well as from an engagement point of view. Evaluation was done against USec principles: visibility (findable), ease of use, satisfaction, effectiveness (is the document secure? confidentiality, integrity, availability to intended users), motivation, comfort, usefulness as well as desirable, understandable, helpful. The overall subjective User Experience metrics were also applied: utility, usability, aesthetics, identification, stimulation and value, based on Section 4.15**.** The review aimed at providing feedback that will inform the design of a user awareness program in the case site and will inform the design of heuristic/metrics for UX with EUPSF in the case site.

The review process also provided important feedback to the building/ development phases by demonstrating the utility of the proposed artefact. Security tasks were performed to evaluate security and experience of experts and peers with the interaction. The findings were used to validate components of the framework which is being developed.

In order to deem a heuristic an important element in the intervention (e.g. awareness program), the heuristic should score more than 5 (33%) on No on a positive aspect; otherwise a 5 is considered on yes, if it is a negative aspect. If a checklist item scores more than 5 on N/A, then it should be taken off the list. This decision was reached after considering benchmark scores for average scores of a popular questionnaire for measuring the perception of usability - System Usability Scale (SUS), which is 68 (Sauro & Lewis, 2012). According to Sauro and Lewis (2012), the average Single Usability Metric (SUM) score is 65%, which is an average of task metrics—completion rates, task-times and task-difficulty ratings.

7.2.6.8 Data analysis

Data analysis was mainly done through data categorisation using predefined themes. Each heuristic is a theme and the data will be analysed under those themes. The first section of the tool captured the demographic information of the evaluators. Their profiles as per completed demographics are presented in Table 7-5.

Table 7-5: Expert and peer reviewer profiles

Reviewer	Qualification	Field of expertise	Gender	Code
1	Dr	Expert IS, Forensics	F	E1
2	Student PhD IS	Expert IS, USec	M	E2
3	Student PhD IS	Expert IS	F	E3
4	Student PhD UX	Expert UX	F	E4/3
5	Dr	Expert HCI	F	E5/4
6	Dr	Expert IS	F	E6/5
7	Prof	Expert IS	M	E7
8	Dr	Expert UX,HCI, USec	M	E8/6
9	Student Honours IS	IS + System admin	M	P1
10	Student Masters IS	IS + System support	F	P2
11	Student Honours IS	IS + System admin	F	P3
12	Student Honours IS	IS + System admin	M	P4
13	Student Honours IS	IS + System admin	F	P5/6
14	Student Honours IS	IS + System admin	F	P6/7
15	Student Honours IS	IS + System admin	M	P6
16	Student Honours IS	IS + System admin	F	P7/8

E3 and E7 did not participate in the Adobe Acrobat Reader evaluation. P6 did not participate in the evaluation of MS Word. The codes of the reviewers will vary according to the application in question owing to the selective participation.

Heuristic evaluation 1 - Adobe: 14 of the 16 participants, comprising four Doctors, two Doctoral students, one Masters student and seven system administrators doing Honours in IS, took part in evaluating Adobe. Among them two are USEC experts, one is a USEC peer, four are InfoSec experts, eight are InfoSec peers, two are UX experts and two are HCI experts. Of these, one is an HCI/USec/UX expert and one is an IS/UX expert.

Heuristic evaluation 2- MS Word: 15 respondents out of the 16 participants. They comprised one Professor, four Doctors, three Doctoral students, one Masters Student and six system administrators doing Honours in InfoSec. Of these, there are two USEC experts, one USEC peer, five InfoSec experts and seven InfoSec peers, two UX experts and two HCI experts. Of these, one is an HCI/USec/UX expert and one is an IS/UX expert.

The discussion of the findings and their impact is presented in summary. Table 7-6 presents a summary of Adobe evaluation.

Table 7-6: Adobe heuristic evaluation

Visibility/Findable/locatable/readily displayed; the security feature must be easily found				
	Yes	No	N/A	Total
Can you easily locate the security feature	9	5	0	14
After completing a security action, do you get some form of feedback	10	2	1	14
Can you disable the security?	10	2	1	14
Motivating- the security feature must encourage users to re- use it again in future				
	Yes	No	N/A	
Are you motivated to use it again?	9	4	0	14
Will you recommend it to others?	10	4	0	14
Does it satisfy your perceived goals?	8	5	0	14
Desirable- the security feature must be pleasant to use, and look at				
	Yes	No	N/A	
Is the presentation visually appealing?	8	3	2	13
Is the feature pleasant to use?	7	4	1	13
Useful- the security features must enable the user to achieve security goals willingly.				
	Yes	No	N/A	
Helps me to be secure	11	3	0	14
They protect my work	11	1	2	14
It does everything I would expect it to do	5	9	0	14
Learnability/understandable, ease of use - the system should ensure that security actions are easy to learn and remember				
	Yes	No	N/A	
The security features have been grouped into logical zones, and headings have been used to distinguish them from other program features	9	4	1	14
I learned how to use the security feature easily	10	4	0	14
The security features are easy to remember	8	6	0	14
Menus make obvious which security items are selected	7	6	1	14
The program protects you from making errors	7	6	0	14
Security-related information is presented in a standardized manner	9	4	0	14
Aesthetics and Minimalist Design; the system should offer users relevant information relating to their security actions				
	Yes	No	N/A	
Only the security information essential to decision-making is displayed on the screen	5	5	3	14
All security icons in a set are visually and conceptually distinct	9	3	2	14
Security labels are brief, familiar and descriptive?	9	5	0	14
Exciting/emotion/perception- the program should promote excitement and good perceptions/ emotions				

	Yes	No	N/A	
You feel excited about the security features	8	6	0	14
You perceive them as good	11	3	0	14
Security tasks evoke positive emotions in you	10	4	0	14
The security-related error messages are accurate in their descriptions	11	2	0	14
It was enjoyable to perform security functions	8	5	0	14
Satisfaction- the system should ensure that users have a good experience when using security and that they are in control				
	Yes	No	N/A	
Security features are easy to work with	8	6	0	14
You feel disturbed when you perform security tasks	2	11	1	14
Security-related prompts imply that you are in control	11	2	1	14
You are satisfied with the security	8	5	0	14
User Suitability - the system should provide options for users with diverse levels of skill and experience in security				
	Yes	No	N/A	
Do the security features support both novice and expert users? Are multiple levels of security error message details available?	5	8	0	14
Can you easily change the level of security detail?	7	7	0	14
Can you easily change between novice and expert levels?	3	9	2	14
Can you customize security to meet your individual preferences?	8	6	0	14
Comfortable to use /User Language -the system should use plain language that users can understand with regard to security				
	Yes	No	N/A	
Are security actions named consistently across all prompts in the program?	8	4	1	13
Is security information accurate, complete and understandable?	8	5	0	13
Are security messages stated in clear and simple language, where used?	8	5	0	13
Is security jargon avoided?	6	6	0	13
User Assistance/ Help - the system should make security help apparent for users				
	Yes	No	N/A	
Is there a security help function visible (e.g. a key labelled “Security Help”)?	6	6	2	14
Is the security information provided relevant?	10	2	2	14
Can users easily switch between security help and their work?	8	5	1	14
Do instructions follow the sequence of user security actions?	10	3	0	14
Does the system provide users with updated security educational opportunities, if they desire it?	3	7	3	14
Efficiency - the security feature must complete the user’s goal in a timely and accurate manner				
	Yes	No	N/A	
Was it easy to enforce security?	5	5	2	14
It takes long to compete the tasks	5	7	2	14
Accessible - the security feature must be reachable to accomplish a security objective				

	Yes	No	N/A	
Does not present technical or physical barriers	11	2	0	14
Readily accessible	10	3	0	14
Effective - the extent to which the security feature fulfils the users' expectations with ease.				
	Yes	No	N/A	
Does what it is supposed to do	9	2	1	14
Fulfils my security needs	8	6	0	14
Usable - the security features must allow the user to do what they want to do in the way they expect to do it without difficulty, hesitancy, or queries				
	Yes	No	N/A	
Is it convenient to use?	9	5	0	14
It is simple to use?	8	6	0	14
Is it doing the expected?	10	3	1	14
Valuable/ impact of use - the security feature should relate to the user goals in a beneficial way				
	Yes	No	N/A	
It secures my documents	10	2	1	14
You are not losing information	8	4	1	14
Your files are not edited by wrong people	9	1	3	14
It does not waste my time	11	1	1	14
It assures you of the file author	8	1	3	14
Security - the system needs to consider integrity, availability, confidentiality, auditing and non-repudiation				
	Yes	No	N/A	
The information is only accessible to authorised users	12	0	1	14
Protected or confidential - can information be accessed only with valid authentication?	12	0	1	14
The program encrypts the whole file	11	1	1	14
You can update or delete document properties' information	9	3	2	14
The program notifies you of your access privileges	8	4	1	14
The program protects all files downloaded	6	2	5	14
Does the program disable macros?	2	5	6	14
Are notification messages relating to security displayed to the user before access to the system is granted?	7	3	2	14
Are the controls for sharing readily available?	6	5	1	14
Does the program install required software updates automatically and notify you about this action?	7	5	1	14
Does the program display options to assist in the reporting of security incidents?	5	5	3	14
Does the program notify you of any vulnerability associated with not applying security?	4	6	3	14
Does the program notify you about auto-recovery?	5	6	2	14
Awareness/Expected - security features must be expected in the programs; users should be aware of their existence				
	Yes	No	N/A	

Does the system provide awareness and educate you on how to complete tasks?	3	10	1	14
Do you expect the security features?	9	3	0	14
Are you aware of the location of the security features in the program?	12	2	0	14
Are you aware of the limitations of the security?	8	6	0	14
Are you aware of the effect of applying security?	14	0	0	14
Are you educated on proper security usage?	10	4	0	14

Heuristic evaluation by both peers and experts established that the security features are:

Visibility: "some security features not that easy to find" as shown by a 36% No response, among those who indicated Yes, some found it difficult to locate the tools. Not easily locatable: "I accessed them through "Tools'. I would of recommended a security tab on the menu too" and one other reviewer commented that it is "very hard to locate looks like with some versions of adobe this is possible only at file creation". Overall, it is visible based on Yes responses. Feedback is not always provided but fairly good. Users can remove the security, "However, in order to complete certain tasks I needed to remove the signature that was done in task", and some found it very difficult to do so.

Motivation: Users are motivated to use some of the features again and to recommend to others, though it does not really support perceived goals (36%);

Desirable: Visual presentation is not so good: "one should have an idea first, it is just displayed in the menu structure." Features are not so pleasant to use (31%). One participant skipped the question.

Useful: It is useful - "it helps me to be secure"; has "better features than Word, but it can still be affected by malicious code", though it does not do everything expected (64%).Respondents feel that their work is protected, although some feel their work would be protected if they had configured all the security actions; they could not complete some of the tasks: "it offers most security features cannot do everything expected of it- it can be removed too easily without verification". "it offers most security features that I would of expected to see but it did not do everything I expected during the configuration of these features"

Learnability/understandable, ease of use: It is generally easy to learn- "it took time to locate it", though some did not find it so easy to learn. They are logically grouped within other program

features such as Edit and Tools; there is no Security heading and it is not clear where to find them. Security features are not so easy to remember, to see which features are selected and the program does not protect users from making errors.

Aesthetics and Minimalist Design: It does not conform to minimalism "There is an overflow of information in certain screens when configuring a security feature. A lot of information can be hidden and displayed when needed by the user". Design and security labels are not really brief, familiar or descriptive.

Exciting/emotion/perception: Respondents do not feel so excited about the security features though they are perceived as good and evoke positive emotions. Features give accurate error messages – "most fairly understandable descriptions". They are not exciting or enjoyable to work with- "it was frustrating and time consuming";

Satisfaction: Generally, it was satisfying; there is no distinction of expert levels though one can customise their security detail. The user language is good, but not comfortable to use; there is poor help or assistance; it is efficient to apply security; it is accessible; effective; usable though not convenient; valuable, though it might waste time for novices. Generally, it is regarded as secure, except for no total encryption; there is no relevant dialogue on security vulnerability associated with not performing security actions; and sharing controls are not readily visible; there is no awareness on security task completion. Table 7-8 summarises MS Word heuristic evaluation.

User Suitability – The system does not provide options for users with diverse levels of skill and experience in security: "they have standard and advanced security options". "Some good descriptions of security features"; however, there is "too much technical oriented terms used to describe the security features" and this will challenge novice users, as there is no other option for them. Users can change the level of security detail moderately, with difficulty.

Comfortable to use: Security actions do not appear multiple times; hence, consistency cannot be evaluated. Reviewer "only noticed the "Protection" and "Sign & Certify" menus in the "Tools" tab. There was no other reference to them in other parts of the program". Security information is not understandable for novices. "Definitely not understandable to users that have no expert security knowledge". Security messages are stated in simple plus technical languages.

User Assistance/ Help: There is no Security Help menu or tab; however "online help" is accessible and the "search bar in help brings up security features". Relevant security information is provided although it is "Difficult to determine without the required security knowledge". Users can switch moderately between security help and their work. The system does not provide users with updated security educational opportunities, if they desire.

Efficiency: It is not easy to complete security tasks and it takes time to complete the task, for both experts and peers.

Accessible: The security features do not present technical or physical barriers depending on the user's ability; for the reviewers it was highly favourable. They are readily accessible "From the perspective of a fully abled user".

Effective: the features are rated as doing effectively what they are expected to do and fulfil the users' needs. However, four of the six experts believe it does not fulfil their security needs.

Usable: Three experts do not agree that the security is convenient to use, even though six of eight peers regard it as convenient. This can pose a serious usability problem for end users. It is simple to use; however, one expert highlights "non IT users will struggle". And mostly reviewers believe the security is doing what is expected.

Valuable/impact of use: It secures users' documents "For features configured successfully". One expert alludes to it as being "too easy to circumvent". Three experts disagree that they are not losing information though "All the information is intact". From the peer point of view, the information is safe. Security features assure users of the file author, although they could not locate the information.

Security: High on access, confidentiality, encryption. The rest of the heuristics fared badly with all experts agreeing that downloaded files are not protected by the program. The program does not disable macros. This is highly risky, as they can be a vehicle for breaching security. Notifications of security are not displayed or applicable, according to five experts. On the contrary, peers see the notifications. Sharing controls are not readily available. There is no: assistance in reporting incidents, education on the risks of not using the security features and notification about auto-recovery.

Awareness/ Expected: Faired well even though the program does not provide the education to users as shown by 11/14 responses. Neither does it explain the limitations of the features explicitly.Generally, the security in Adobe is moderate to good, based on the review. It would have been helpful if all reviewers had filled in the extent per checklist item; however, limited feedback in that regard is provided, making it extremely difficult or impossible to calculate the difficulty levels. However, there are critical areas that need to be focused on to improve the usability. Using awareness as a vehicle, experts in the organisation could evaluate what impacts the security in line with organisational security values; and could focus on those in the intervention program. The completed extents of task usability complexity are reflected in Table 7-7. They are rated from very difficult (1) to very easy (5) per heuristic checklist item. Column 1 is the heuristic and the next column is the checklist item for the heustic in question.

Table 7-7: Summary of extents of usability per item

		1 very difficult			2 difficult		3 moderate			4 easy		5 very easy	
Heuristic	**Checklist item**	**Y**	**N**	**N/A**	**Y**	**N**	**Y**	**N**	**N/A**	**Y**	**N**	**Y**	**N**
2	1. A	-	-	-	1	1	1	-	-	1	-	3	-
	2. B	-	-	-	-	-	2	-	-	1	-	1	-
	3. 3	-	-	1	-	-	2	-	-	2	-	1	-
3	1. 1	-	-	1	1	1	1	-	-	1	1	-	-
	2. 2	-	1	-	-	-	2	-	-	1	1	-	-
	3. 3	-	-	-	1	1	1	1	1	-	1	-	-
4	1.	-	-	-	-	-	2	1	-	2	-	-	-
	2.	-	-	-	-	1	1	1	-	2	-	-	-
5	1.	-	-	-	-	-	3	-	-	1	-	-	-
	2.	-	-	-	-	-	2	-	-	2	-	-	-
	3.	-	-	-	-	1	1	2	-	-	-	-	-
6	1.	-	-	-	-	1	1	-	-	1	-	2	-
	2.	-	1	-	-	-	4	-	-	2	-	1	-
	3.	-	1	-	-	1	3	-	-	2	-	1	-
	4.	-	-	-	-	2	-	-	-	2	-	1	-
	5.	-	1	-	1	-	2	-	-	1	-	1	-
	6.	-	-	-	2	1	1	-	-	1	-	1	-
7	1.	-	1	-	1	-	1	1	-	-	-	1	-
	2.	-	-	-	-	-	2	-	-	2	-	1	1
	3.	-	-	-	-	-	2	-	-	2	-	1	-
8	1.	-	-	-	-	1	1	-	-	1	1	1	-
	2.	1	-	-	-	-	1	-	-	2	-	1	-
	3.	-	-	-	-	-	1	1	-	1	-	1	-
	4.	-	-	-	1	-	3	-	-	-	-	1	-
	5.	-	-	-	-	1	-	-	-	1	-	1	-
9	1.	-	-	-	2	2	-	-	-	1	-	-	-
	2.	-	-	-	-	-	1	-	-	-	-	-	-

		1 very difficult			2 difficult		3 moderate			4 easy		5 very easy	
Heuristic	**Checklist item**	**Y**	**N**	**N/A**	**Y**	**N**	**Y**	**N**	**N/A**	**Y**	**N**	**Y**	**N**
	3.	-	1	-	1	-	-	1	-	1	-	-	-
	4.	1	1	-	-	-	-	-	-	1	1	-	-
10	1.	-	1	-	1	-	-	2	-	-	-	1	-
	2.	-	1	-	1	-	2	1	-	1	-	1	-
	3.	1	1	-	-	-	-	1	-	-	-	1	-
	4.	-	-	-	-	-	1	1	-	1	-	2	-
11	1.	-	-	-	-	1	1	-	-	2	-	1	-
	2.	-	1	-	1	-	-	1	-	2	-	1	-
	3.	-	1	-	-	-	2	1	-	1	1	1	-
	4.	-	1	-	-	-	-	2	-	1	-	1	-
12	1.	-	-	-	-	-	2	-	-	-	1	-	-
	2.	-	-	-	1	-	-	-	-	3	-	-	-
	3.	1	-	-	-	-	2	-	-	1	-	-	-
	4.	-	-	-	1	-	-	1	-	2	-	-	-
	5.	-	-	-	-	1	1	-	-	-	-	-	-
13	2.	-	-	-	-	1	1	1	-	1	-	-	-
	3.	-	-	-	1	-	-	1	-	-	-	-	-
14	1.	-	1	-	3	-	-	-	-	1	-	-	-
	2.	-	-	-	1	-	3	-	-	-	-	-	-
15	1.	-	-	-	-	-	2	1	-	1	-	-	-
	2.	-	2	-	-	-	-	1	-	1	-	-	-
16	1.	-	1	-	-	-	2	1	-	1	-	1	-
	2.	-	1	-	1	-	1	-	-	1	-	2	-
	3.	-	-	-	-	1	1	-	-	1	-	2	-
17	1. 1	-	-	-	-	1	1	-	-	1	-	-	-
	2.	-	-	-	-	1	-	-	-	1	1	-	-
	3.	-	-	-	-	1	-	-	-	1	-	1	-
	4.	1	-	-	-	-	3	-	-	1	-	-	-
	5.	-	1	-	-	-	1	-	-	1	-	-	-
18	1.	-	-	-	1	-	2	-	-	2	-	-	-
	2.	-	-	-	1	-	2	-	-	2	-	-	-
	3.	-	-	-	-	-	2	-	-	1	-	-	-
	4.	-	-	-	-	-	3	-	-	1	-	-	-
	5.	-	-	-	-	1	2	-	-	1	-	-	-
	6.	-	-	-	1	-	1	-	-	-	-	-	-
	7.	-	-	-	-	1	-	-	-	-	-	-	-
	8.	-	-	1	1	1	1	-	-	-	-	1	-
	9.	-	-	1		-	1	1	-	-	-	1	-
	10.	-	-	-	1	-	-	1	-	-	1	-	-
	11.	-	1	-	-	-	-	1	1	-	-	-	-
	12.	-	1	-	-	-	-	1	-	1	-	-	-
	13.	-	1	-	1	-	-	1	-	-	-	-	-
19	1.	-	1	-	-	-	2	2	-	-	-	-	-
	2.	-	-	-	-	1		1	-	1	-	-	-
	3.	-	-	-	1	-	2	1	-	1	-	-	-
	4.	-	1	-	-	-	-	-	-	-	-	1	-
	5.	-	-	-	-	-	1	-	-	3	-	-	-
	6.	-	-	-	-	-	1	1	-	-	-	2	-

Microsoft Word

Table 7-8 is a summary of the heuristic evaluation conducted on MS Word security features.

Table 7-8: Word heuristic evaluation

Visibility/Findable/locatable/ readily displayed – the security feature must be easily found					
Checklist Items	Yes	No	N/A	Total	Others
Can you easily locate the security feature?	12	3		15	
After completing a security action, do you get some form of feedback?	12	3		15	
Can you disable the security?	9	4		14	1 not sure
Motivating- the security feature must encourage users to re-use it again in future					
Checklist Items	Yes	No	N/A	Ext	
Are you motivated to use it again?	10	5		15	
Will you recommend it to others?	12	3		15	
Does it satisfy your perceived goals?	11	3	1	15	
Desirable– the security feature must be pleasant to use, and look at					
Checklist Items	Yes	No	N/A	Ext	
Is the presentation visually appealing?	9	6		15	
Is the feature pleasant to use?	9	5		15	1 Ext 3
Useful - the security features must enable the user to achieve security goals willingly.					
Checklist Items	Yes	No	N/A	Ext	
Helps me to be secure	12	2	1	15	
They protect my work	14		1	15	
It does everything I would expect it to do.	7	7	1	15	
Learnability/ understandable, ease of use – the system should ensure that security actions are easy to learn and remember					
Checklist Items	Yes	No	N/A	Ext	
The security features have been grouped into logical zones, and headings have been used to distinguish them from other program features	13	2		15	
I learned how to use the security features easily	11	4		15	
The security features are easy to remember	12	2	1	15	
Menus make obvious which security items are selected	10	4	1	15	
The program protects you from making errors	5	8	2	15	
Security-related information is presented in a standardized manner	8	5		15	1 I don't know, 1 not sure
Aesthetics and Minimalist Design – the system should offer users relevant information relating to their security actions					
Checklist Items	Yes	No	N/A	Ext	
Only the security information essential to decision making is displayed on the screen	10	3		14	1 I don't know
All security icons in a set are visually and conceptually distinct	8	6		15	1 ext 3
Security labels are brief, familiar and descriptive	12	3		15	
Exciting/emotion/perception – the program should offer excitement and good perceptions/ emotions					
Checklist Items	Yes	No	N/A	Ext	
You feel excited about the security features	6	6	3	15	
You perceive them as good	12	2	1	15	
Security tasks evoke positive emotions in you	8	4	2	15	
The security-related error messages are accurate in their descriptions	11	3		15	1 ex 4
It was enjoyable to perform security functions	9	3	2	15	1 ext3
Satisfaction – the system should ensure that users have a good experience when using security and that they are in control					
Checklist Items	Yes	No	N/A	Ext	

Security features are easy to work with	9	4		15	
You feel disturbed when you perform security tasks	3	12		15	
Security-related prompts imply that you are in control	9	4	1	15	
You are satisfied with the security	11	2		14	1 ext 3
User Suitability – the system should provide options for users with diverse levels of skill and experience in security					
Checklist Items	Yes	No	N/A	Ext	
Do the security features support both novice and expert users? Are multiple levels of security error message details available?	7	7	1	15	
Can you easily change the level of security detail?	7	6		15	1 ext 2, 1 ext 4
Can you easily change between novice and expert levels?	3	8	3	15	1 ext 2
Can you customize security to meet your individual preferences?	11	4		15	
Comfortable to use /User Language – the system should use plain language that users can understand with regard to security					
Checklist Items	Yes	No	N/A	Ext	
Are security actions named consistently across all prompts in the program?	10	5		15	
Is security information accurate, complete and understandable?	10	4	1	15	
Are security messages stated in clear and simple language, where used?	10	5		15	
Is security jargon avoided?	9	5		14	
User Assistance/ Help – the system should make security help apparent for users					
Checklist Items	Yes	No	N/A	Ext	
Is there a security help function visible (e.g. a key labelled “Security Help”)?	4	11		15	
Is the security information provided relevant?	11	2	2	15	
Can users easily switch between security help and their work?	8	4	3	15	
Do instructions follow the sequence of user security actions?	9	5	1	15	
Does the system provide users with updated security educational opportunities, if they desire it?	3	9	3	15	
Efficiency - the security feature must complete the user’s goal in a timely and accurate manner					
Was it easy to enforce security?	9	4		14	
It takes long to compete the tasks	6	7		14	
Accessible – the security feature must be reachable to accomplish a security objective					
Checklist Items	Yes	No	N/A	Ext	
Does not present technical or physical barriers	12	2		14	
Readily accessible	10	4		14	
Effective - the extent to which the security feature fulfils the users’ expectations with ease.					
Checklist Items	Yes	No	N/A	Ext	
Does what it is supposed to do	13	1	1	15	
Fulfils my security needs	11	2	1	15	1 ext 4
Usable - the security features must allow the user to do what they want to do in the way they expect to do it without difficulty, hesitancy, or queries					
Checklist Items	Yes	No	N/A	Ext	
Is it convenient to use?	12	3		15	
It is simple to use?	13	2		15	
Is it doing the expected?	13	1	1	15	
Valuable/ impact of use – the security feature should relate to the users’ goals in a beneficial way					
Checklist Items	Yes	No	N/A	Ext	

It secures my documents	14			14	
You are not losing information	12	1		14	1 I don't know
Your files are not edited by wrong people	12	1	1	14	
It does not waste my time	8	4	2	14	
Assures you of the file author	7	4		11	
Security – the system needs to consider integrity, availability, confidentiality, auditing and nonrepudiation					
Checklist Items	Yes	No	N/A	Ext	
The information is only accessible to authorized users	12	1	1	14	
Protected or confidential information can be accessed only with valid authentication	13		2	15	
The program encrypts the whole file	9	5	1	15	
You can update or delete document properties information	13	1	1	15	
The program notifies you of your access privileges	11	2	2	15	
The program protects all files downloaded	7	5	2	15	1 I don't know
Does the program disable macros?	5	7	3	15	
Are notification messages relating to security displayed to the user before access to the system is granted?	10	2	2	15	1 ext 3
Are the controls for sharing readily available?	9	5	1	15	
Does the program install required software updates automatically and notify you about this action?	6	6	2	15	
Does the program display options to assist in the reporting of security incidents?	6	8	1	15	
Does the program notify you of any vulnerability associated with not applying security?	4	11		15	
Does the program notify you about auto recovery?	8	6		14	
Awareness/Expected security features must be expected: the programs, users should be aware of their existence					
Does the system provide awareness and educate you on how to complete tasks?	3	11	1	15	
Do you expect the security features?	12			14	2 question not clear
Are you aware of the location of the security features in the program?	13	2		15	
Are you aware of the limitations of the security?	8	7		15	
Are you aware of the effect of applying security?	15			15	
Are you educated on proper security usage?	11	4		15	

The heuristic evaluations reflect the following:

Visibility: Security feature are easy to locate, although "some features were easier to locate than others (E4)"; and (E6) agrees. "Restricting editing not possible on my Mac because I am the only user on it (E5)". 'Some of them like password protect (E3)" are not easy to locate; it is "not too

clear where one can find the security features (E8)". Feedback is available after completing tasks, but "feedback is difficult to understand though (E8)'. Security can be disabled; however, "I did not receive or at least did not notice any feedback when disabling the security" and "Not all security features could be disable password (E8)", One expert found the question confusing. As such, clarity needs to be added to the tool for future evaluations. "Not sure what this question means? Disable security on the document or disable security features in the application? (E5)."

Motivation: It is partial, as some who said "yes' went on to qualify, i.e. "some of the security features", "I will probably just use the password feature to control access to the document. Other features are just too difficult to apply correctly (E8)". The security features can be recommended to others as they achieve perceived goals, but "for user who don't understand digital certificates. The encryption feature is not recommendable (E3)".

Desirable: Visual presentation is not so good "visual appearance is lacking. The use of images could contribute more to understanding the purpose of a security feature (E8)" Features are moderately pleasant to use.

Useful: Useful, although E1 cites that it is "easily broken" and, according to E8,"I was only confident that I did the password protection correctly. All other tasks completed I am not confident that they were configured correctly". The features protect the user's work. "I feel that if I had configured all the security actions correctly that my work would be protected. But the knowledge time and effort needed to configure all those features correctly is overwhelming" (E8). However, the security does not do everything expected of it.

Learnability/understandable, ease of use: They are logically grouped within other program features, such as Edit and Tools; there is no security heading and it is not clear where to find them. "Not at all logical to me where some features are located (E3)". The program does not protect users from making errors. "When creating the password I was not able to view the characters that I was typing in. I could have easily made a mistake. Furthermore it did not give me automatic feedback as to whether I had a strong or weak password (E4)".

Aesthetics and Minimalist Design: The security features do, to a greater extent, conform to minimalist design.

Exciting/emotion/perception: "Useful but not exciting" E1 summarises the responses; "I do perceive them as good if I knew how to configure them" (E8). "I did feel positive emotions when I configured the password protection just as I felt negative emotions when I could not configure the other features correctly", as summarised by (E8). Emotions are not always positive, as "Not always I was unaware of how to set the read only feature on and therefore found it frustrating. I eventually had to watch a help video which was time consuming. Negative emotions were experienced here" (E4). Other users experience the same challenges. Error messages are accurate in their descriptions, but "Difficult to understand". "Overall yes"; the tasks invoke positive feelings.

Satisfaction: Generally satisfying; they are easy to work with; important to reviewers; they do not feel disturbed; security prompts do not always imply that the user is in control, "The prompts provided in some cases do not imply that I am in control (e.g. I cannot return and edit the details of a digital certificate before I actually add the digital certificate to the document" (E8).

User Suitability: The system does not provide options for users with diverse levels of skill and experience in security. All experts, but one, agree that security features do not support both novice and expert users and feel that there are no multiple levels of error message detail available. E6 chose Not Applicable, which infers that the functionality is not available and this is confirmed by a walkthrough of the features. On the contrary, all peers believe it is supported. To ensure that users use the features, their skills need to be upgraded to acceptable levels, as there is "only one level available" E5.

Comfortable to use: Comfortable, although a lot of technical jargon is used; end users (novices) may not understand it.

User Assistance/ Help: No; however, the EUP help function incorporates security help functionality, as indicated by E5: "Help search bar brings relevant functions". Relevant security information is provided. The system does not provide users with updated security educational opportunities, if they desire.

Efficiency: It is easy to enforce the security, for all experts who answered; however three rated usability at 3. E1 says yes, E4 "overall yes" - this implies inherent difficulty. E3 rated it as very easy. On the peer side, more than half (4) did not find it easy. Considering that peers are closer to

end users, and even experts raised concerns, the feature is not so easy to use. It creates a barrier for the user.

Accessible: The security features do not present technical or physical barriers. Readily accessible as 10/14 respondents indicated Yes.

Effective: the features are rated as doing effectively what they are expected to do and fulfilling the user's need.

Usable: They are very usable for peers; fourof the seven experts share the same view.

Valuable/impact of use: It secures users' documents. Security assures users of the file author. "You have the ability to restrict access to certain people in a domain, assuming it is configured correctly" (E8). "It does require a lot of time to learn to configure" (E8), "Only if you know how to use the feature then you don't waste time" (E3), although it is "Difficult to figure out which feature to use. Not all features are in the same menu" (E7). Security is valuable; therefore is not considered to waste time; however,it requires a lot of time to learn, to figure out which feature to use as features are not in the same menu and users need to know where to find them. There is a need for EUA.

Security: High on access and confidentiality. "Not evident if the entire document is encrypted" (E8). Some believe yes; some no. The feature Help does not specify the extent of the application of the security; security is placed on keeping the password. Interestingly enough, end users are encouraged to keep a list of passwords and corresponding document names. Question: Are the documents secured or it is just an extra task to perform that results in a breach of security best practices? Controls and notifications are good. The rest of the heuristics fared badly. All experts agree that downloaded files are not protected by the program. Sharing controls are not readily available. There is no: assistance in reporting incidents; education on the risks of not using the security features; and notification about auto-recovery. Auto recovery - Most experts said No (5/8), 1/8 said yes, but "You need to be aware of this feature": only two agree; however, all but one peer agree that the program notifies.

Awareness/ Expected: All experts agree that there is no security feature awareness or education offered by MS Word. The security features are expected in the program; however, two experts

found it difficult to understand the expectation of the question. For future use, the question needs to be clarified, i.e. Do you expect the security features in the program? Awareness of the feature location is excellent, although twoexpert said it is "not all easy to locate" (Expert 6) and "Not easy to locate though" (E8). All reviewers are aware of the implications of applying the security, although five experts out of eight are not aware of the security limitations. The participants are trained from other sources; not the EUP. There is a need to educate users on the features in programs implemented in the organisation. The software does not educate or assist users on security usage (E8).

Generally, the security in MS Word is usable based on the review; however, there are areas of concern that need organisational experts to address in order for user experience of these features to be positive. In a similar study, a major obstacle for end users to the use of EUPSF was found to be their usability (Furnell, 2005).The importance of empowering end users to protect themselves was highlighted, and usability problems were identified in terms of finding, understanding, and ultimately using the security features, using Microsoft Word as an example (Furnell, 2005). It would have been helpful if all reviewers had filled in the extent per checklist item; however, limited feedback in that regard is provided making it extremely difficult or impossible to calculate the difficulty levels.

7.2.6.9 Reporting - Result interpretation

The usability of security features in MS Word and Adobe Reader are moderate to good, although the user experience is on the low side. The features achieve their goals, although they place a burden on the user. For instance, the features are not so easy to locate, i.e. "are not easy to locate; it is "not too clear where one can find the security features (E8)"; "Signature can be digital signature or a signature image. Had to google digital signature in the latest Word for Mac version as I used it before on different Word version- discovered it is not provided for (E5)". This puts a burden on the reviewers, as they need to go out of their way to find them. In some cases the user has to go on the Internet to get the help they needed to complete the security task. This gives negative emotions about the feature and can deter the usage of it. For example, E4 said: "Not always I was unaware of how to set the read only feature on and therefore found it frustrating. I eventually had to watch a help video which was time consuming. Negative emotions were experienced here" answering to the checklist item "Security tasks evoke positive emotions in

you". The result confirms that, contrary to the assumption, security features are not so usable and result in negative user experience, even for security interested and experienced expert users. UX was measured by usability, emotions and attitudes associated with task execution. Based on these findings, awareness and training on security features is vital to improving security and user experience of interaction with EUPSF. The cross comparison of MS Word vs Adobe heuristics on a checklist basis is presented in Appendix B3.

7.2.7 Expert review: Tentative framework evaluation

Experts from the InfoSec, IS and HCI fields were identified and approached to evaluate the framework development process.

Informed argumentation demonstrates whether the framework development process conforms to existing standard methods or not (Oates, 2012). The framework development process followed a tested and proven method for information systems, behavioural and artefact development, design science research. Literature sources were augmented to justify the stages of the process.

The expert validation was undertaken through document review by field experts. A detailed outline of the framework development process, the framework components, plus their validation and the resultant framework, were sent to five experts in total. The experts are from the fields of HCI (1), InfoSec (3) and IS (1). Four of the experts returned written comments, and they were all involved in a discussion. The HCI expert was engaged via Skype to explain his concerns and to give clarification on some of the written feedback as he is based in South Africa. Three local experts (two InfoSec and one IS) were engaged in a group discussion also, where the researcher presented the process and they commented. The comments were audio-recorded and noted on paper. The fifth InfoSec expert is from the USA, but was on contact during the write-up and thus was also verbally engaged on their feedback.

The experts critiqued the development process on consistency to the design science research method, which was followed and the feedback was used to refine the process. The comments were made on a section basis; this made it easier to address them. The process was also validated against four other framework development processes. All of this was done to demonstrate the rigour of the development method.

7.3 REFINED EUPSFUX FRAMEWORK

The framework underwent reviews by five experts in the fields relevant to the framework. Table 7-9 provides an overview of the expert demographics.

Table 7-9: Expert demographics

Reviewer	Qualification	Field of expertise	Gender	Code
1	Dr	Expert Information Systems	M	ER1
2	Student PhD InfoSec	Expert InfoSec, USec	M	ER2
3	Student PhD InfoSec	Expert InfoSec	F	ER3
4	Dr	Expert HCI	F	ER4
5	Dr	Expert IS, Forensics	F	ER5

Based on the evaluation and validation processes, Table 7-10 presents the identified areas of improvement by experts. Experts ER1 and ER2 gave comments that influenced the change in the framework while the rest commented on alignment and terminology used, e.g. the use of the word evaluation vs. assessment.

Table 7-10: Framework development process evaluation

Evaluation criteria	Expert	Proposed improvement	Improvement made
Utility	ER1	Who are the target users of the framework? • Why will they use the framework? • How will they use the framework? • What will they achieve from using the framework?	Stakeholders clearly defined. Roles of stakeholders explained. Demonstrated through a use case scenario. Demonstrated through a use case scenario.
Utility and validity	ER2	Key aspects that come into play here include: your methodology, your target community, the literature section and the findings.	The phases are applied to the development process and the stakeholders are defined.
Completeness ER1	ER1	How do evaluation, derivation and implementation guidelines of the framework link?	Components are related clearly in the framework.
		Is this an implementation guideline helping the practitioner on how to use the framework?	Explicitly explained in the framework description
Completeness	ER2	I would think there are data and findings which could have helped in coming up with this framework. Refer to those mentioned sections.	Reference has been made to supporting data.
Ease of use	ER1	The framework is a bit dense and difficult to follow. I suggest putting in the abstract components; then unpack them in the description of the framework	The framework was refined to be lighter and clearer as in Figure 7-1.
General	ER5 ER1	Formatting of the diagram to align the components. Colours and text should blend well.	
Validity	ER1	Refer to theoretical framework and relate to empirical study	Addressed in the design process.
		Clarify the evaluations in the framework. How does the first one relate to the second one? Too early to evaluate change the wording, i.e. assess	Changed in the framework and explained.

Based on the critical reviews of the experts, the feedback was incorporated to finalise a refined framework. Figure 7-1 represents the refined framework.

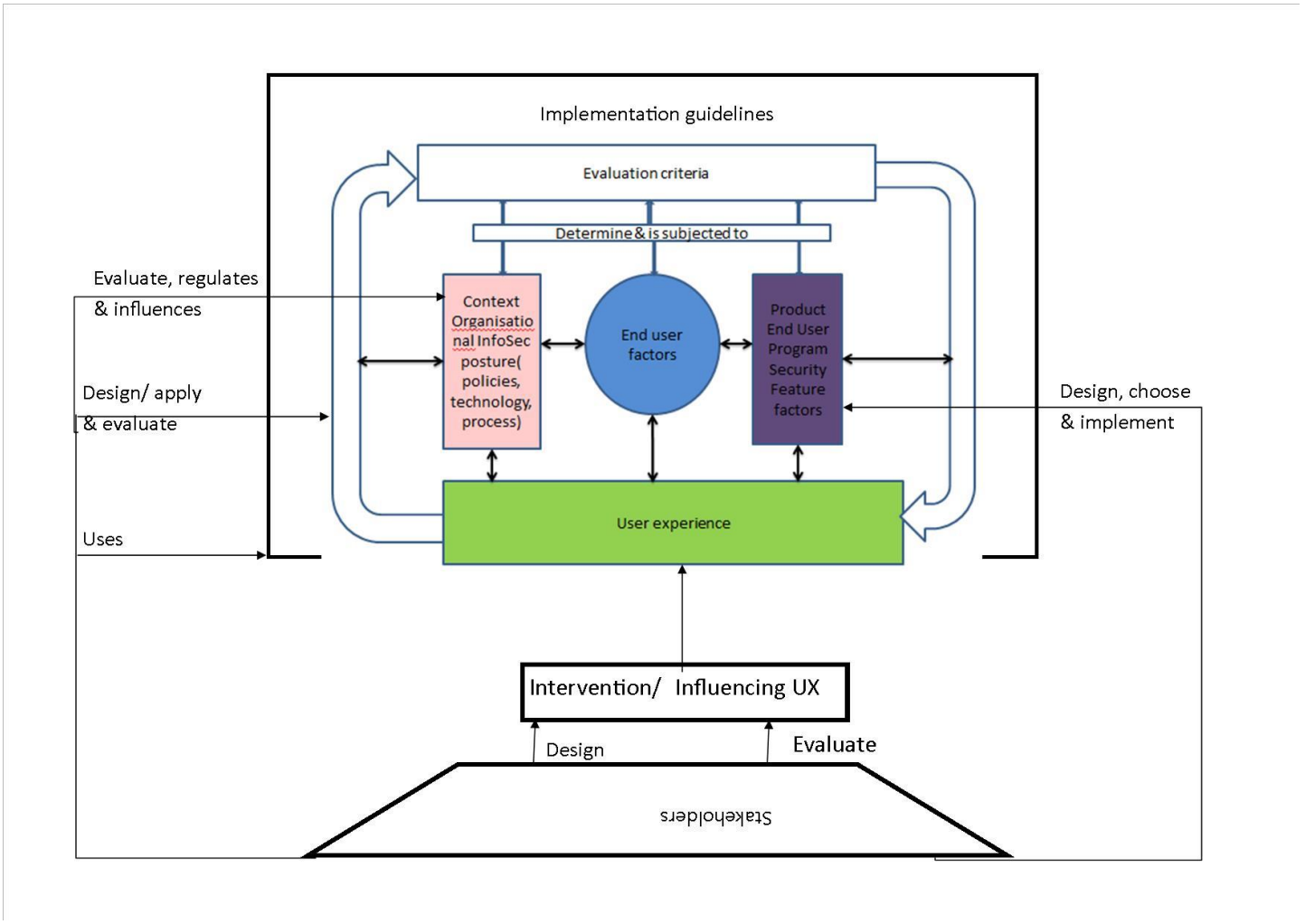


Figure 7-1: Refined framework

The original framework, Figure 6-19, is suitable as a demonstration of the applicability of the implementation guidelines as it positions all components relative to one another with typical data. The framework demonstrates that EU characteristics/ factors are the centrepiece of the UX evaluation and influencing in EUP and can influence the security posture of the organisation at large. Identified metrics speak mainly to the EU characteristics especially awareness. The EUPSF as a technology supports the EU to have positive experiences while using ICTs for their work using EUP.

Organisational security culture drives and influences EU interaction with EUPSF hence UX can be contextual, this is to a large exnt depended on the human aspect as they are responsible for designing policies and selecting the right EUP for employees.

7.4 FRAMEWORK LIMITATIONS

The areas of user behaviour and organisational culture were not addressed because of the scope of the study. Heuristic studies were conducted by peers and experts. It would have been interesting to compare the findings with user studies on the same scope. The framework was not implemented and evaluated in real use. The study was conducted in one site; a cross site evaluation would have improved the generalisability of the framework. The heuristic list is very long and that deterred most of the consulted experts from completing the evaluation.

7.5 SUMMARY

This chapter presented the tools, processes and a guideline developed in the research and positions them as contributions to the body of knowledge and industry practice. The quality of the framework was demonstrated by demonstrating: transferability through documentation of the tools and methods which were used in designing and validating the EUPSF; credibility by using data and method triangulation; confirmability though the use of clearly outlined methods and processes for data collection and analysis as wel as use of literature to confirm findings. The reliability of the study was demonstrated through bias elimination in the administration (self) of the survey as well clear documentation of research methods and strategies.

EUPSF were validated through task-oriented heuristic evaluations by peers and experts in the HCI, InfoSec, USec and UX fields in two different case programs using a multiple case study strategy in line with the eight heuristic evaluation stages. The heuristic evaluation eight stages are: planning, selecting evaluators, selecting the program to evaluate, determining a set of heuristics to evaluate, prepare to collect data, developing tasks for evaluators, conducting the evaluation and finally, analysing the data.

Using the comments of the experts on the framework development process presented in Table 7 10 on the tentative framework and its development process, a refined framework was designed and is presented in Section 7.3, Figure 7.1.

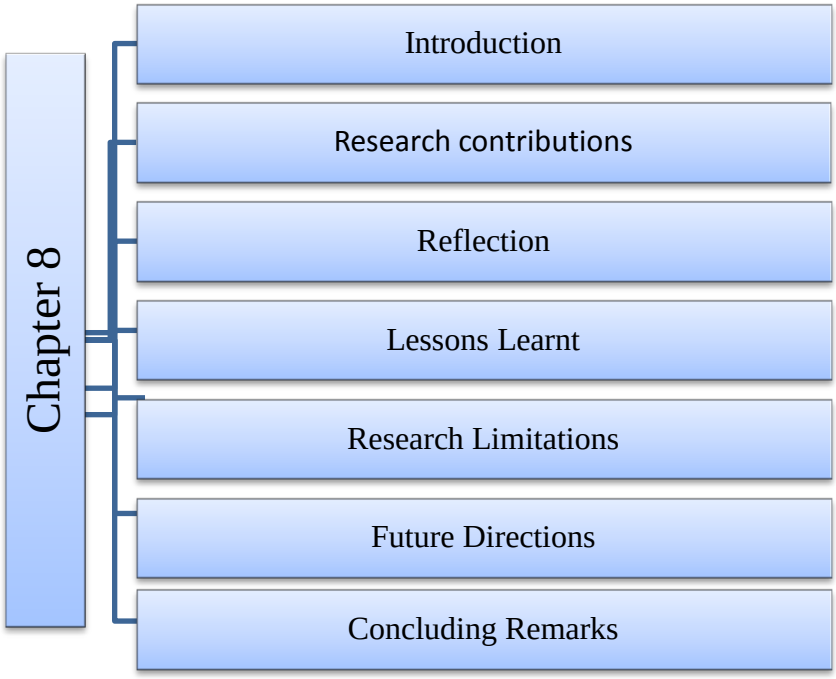
CHAPTER 8: OVERALL RESEARCH CONCLUSION

8.1 INTRODUCTION

The previous chapters discussed the problem, methodologies, literature studies, as well as the empirical study, the framework design and evaluation. The research problem was identified as the lack of user experience evaluation criteria (metrics) to assess the user's experience of interacting with embedded security features in end user application programs. A framework for evaluating UX of security features in EUPs, which integrates organisational InfoSec culture, end user characteristics and EUP security features into a UX metric, was developed. The proposed framework is in line with the main goal of this research work. It is envisaged that the developed security UX framework will make available a platform for testing and ensuring that application security does not only provide security to information, but also a secure and positive experience. This will encourage users to make informed use voluntarily of embedded security features in their programs and will, in turn, improve personal and organisational information security. In so doing, the framework will address the following gaps which were identified from the literature review:

1. Lack of tools to evaluate UX with application security features
2. Lack of metrics to measure awareness levels of case subjects.

The study adds to the literature in the area of UX evaluation and measurement, in general, and specific to end user program security. The research contributes to the theoretical body of knowledge within the information security and user experiences' sub-domain of human Computer Interaction on securing end user program security features. It also creates a platform for further academic research on human factors of information security and user behaviour. This chapter presents the researcher's view of the whole thesis, following the outline.



Reflection, lessons learnt, research limitations, future directions and concluding remarks are presented in the following sections. First, the next section presents an overview of the research contributions.

8.2 RESEARCH CONTRIBUTIONS

From the research it was established that there are no tools and mechanisms to evaluate UX experience with EUPSF; hence, the need exists to develop a framework to address the gap. This thesis contributes to the body of knowledge of InfoSec and UX elements of HCI on how user behaviour can be influenced for positive UX with InfoSec. This study has identified factors that affect UX with end user program security features. Secondly, metrics which can be used to evaluate user awareness of security features and UX with interaction with security features embedded in end user programs were identified and developed. Thirdly, the framework presents the components and the relationships that exist between the components themselves and their impact on UX of interacting with embedded end user security features. During the process of answering the research questions guiding this study, the following can be noted:

From the literature review and case site document analysis, the following shortcomings were identified:

1. The lack of a security awareness program at the case site. Thus as a result there is a need for the creation of security awareness programs to be implemented with the view of communicating with institutional policies and best practices.
2. The lack of specific metrics for establishing baseline security awareness among end users.
3. The lack of an integrated view of security and user experience components.

In response to the shortcomings, answers to the research questions and the case study, the following contributions to the body of knowledge can be recorded:

1. A theoretical framework showing the components of the research topic and their relationships (Section 5.5.3, Section 6.3.3.3).
2. The identification of security and UX issues affecting end users with application programs (Section 5.5.2).
3. Metrics for establishing baseline security awareness among end users (Section 5.5.4).
4. A model showing the relationships between the InfoSec and UX aspects and user behaviour. This also provided a new approach to addressing environmental aspects on security behaviour (Section 5.5.3).
5. Metrics for evaluating UX of interacting with application programs using a heuristic evaluation (Section 7.2.6).
6. An incremental framework development process for developing and evaluation of the EUPSFUX framework (Section 6.3).
7. A framework (EUPSFUX) for evaluating the UX of interacting with embedded security features in end user application programs (Section 6.3.5.5).
8. Framework implementation guidelines to guide the implementers at insitutional level (Section 6.3.3.4).
9. A theoretical framework showing the components of the research topic and their relationships, an output of the literature review.
10. The identification of security and UX issues affecting end users with application programs, as published in Paper 1. Answered Research Question 1 using literature reviews and empirical studies (Appendix C1).

11. Metrics proposed for establishing baseline security awareness among end users, as published in Paper 2 and Cambridge book, Chapter 10. This was in part answering Question 2, on identifying the UX metrics for EUPSF (Appendix C2 & 3).
12. A need was identified for security awareness programs to be implemented in an academic institution aimed at communicating policies and best practices.
13. The research adds to the literature in the area of UX evaluation and measurement, in general, and specific to end user program security features.
14. A platform was created for further academic research on human factors of information security in end user programs.

Specific novel contributions to the body of knowledge are discussed in the following sections.

8.2.1 Contribution 1: Framework design process

A framework design process guided the research process as it informed every stage of the framework development and related it to the research methodology applied to the case study. The process was based on a review of design science frameworks applicable to information systems.

Benefits

It allows for the framework to be validated for rigour as it can be evaluated for the reliability of the method applied in developing the EUPSFUX framework.

8.2.2 Contribution 2: Framework implementation guideline

The process allows for stakeholders (practitioners) to apply the framework in context and to collect actual measures of UX at any given time.

Benefits

The process can be followed systematically and is based on theoretical foundations as the design was informed by literature reviews.

8.2.3 Contribution 3: EUPSFUX framework

The framework is based on the three critical components that should be present in every business model for information security (BMIS) and user experience. The components are: people

(referred to as stakeholders in this study and end users in UX), technology (product in UX which, in this study, is the security feature in a EUP (in particular MS Word and Adobe acrobat Reader)) and organisation strategy (context in UX which, in this case. is the organisational InfoSec culture). The framework focuses on the human factors as a dynamic interconnector between people and technology. UX occurs as a result of human and technology factors and is dependent on human factors and technology factors in context. The technology is end user security features in the context of MS Word or Adobe Acrobat Reader as used at PoN. The people aspect defines program end users, InfoSec experts, UX experts and IT technical experts (team). The critical components allow for information security and UX to be evaluated at three levels, namely: people, technology and context. Level 1 is identifying EUPSFUX factors through user studies, context analysis and focusing on particular products. At level 1, the experts are evaluating the critical components. Level 2 entails establishing a baseline of the identified factors by evaluating InfoSec, EU, UX and EUPSF factors, using user studies, heuristic evaluation and security awareness baseline metrics. This is also done by the experts. Level 3 is influencing UX change; this is done by developing an intervention that is context sensitive as it is influenced by factors identified in the environment of application. In this instance, there was no user awareness program in place; hence, that is recommended as the first strategy for influencing positive and secure UX. Depending on the posture of the context and culture, a change management programs might be necessary to influence user behaviour. The rest entails re-evaluating and maintaining or influencing the UX for better organisational security.

Benefits

The framework allows for user experience of end user interactions with end user program security features to be evaluated in a context-sensitive manner.

8.2.4 Contribution 4: Framework evaluation toolset

Measures EUPSF usability, security and UX done using heuristic evaluation security awareness metrics. The next two sections present the tools in detail.

8.2.5 Heuristic evaluation

End User Program (EUP) USec, UX and security heuristics with associated checklist items, were developed and applied to MS Word and Adobe Acrobat Reader. The heuristic evaluation is

specific to end user program; however, can be varied on a task-specific basis to match the inherent security functionality and features in the program under review. The heuristics are used as criteria to identify security, usability and user experience violations during interaction with an EUP. It allows for InfoSec, IT team and UX experts in organisations to identify areas of concern; to train end users on best practice and to achieve organisational security and positive user experience.

Benefit

Informed intervention to improve end user interactions with EUPSF, user perceptions and attitudes towards security features, positive user experiences and behaviour, and an overall secure organisation can be achieved.

8.2.6 Awareness metrics

Measures for evaluating security awareness levels in context were generated. Awareness survey, user behaviour and computer infections were identified as awareness metrics.

Benefit

They allow for practitioners (UX, IT team and InfoSec experts) to establish the UX and security posture of the organisation before taking any action.

8.3 REFLECTION

This section presents a reflection on the relationship of the expected product of the research process, the research problem and the contributions made. The research paradigm, DSR has reflection as the third cognitive process that is carried out before concluding the research (Vaishnavi & Kuechler, 2004). Three types of reflection will be presented, namely: scientific, methodological and substantive

8.3.1 Methodological reflection

Focus is placed on the appropriateness of the applied research methods, paradigms and processes. The problem-based research cycle, as well as design science research, was chosen for the study. The problem-based research was used to identify the problem, set the research objectives and identify the research methodology. Problem identification fits with stage 1 of DSRM; and the determination of research objectives and question fits with stage 2 of DSRM. Stage 3 of DSRM speaks to design and development of a solution; however, there is a need for a

clear methodology to be defined which, when followed, can lead to the artefact development, as such problem-based research in a case study setup was used to complement DSRM in this aspect. After determining the methodology, problem-based research was silent on how one can go about solving the problem and this is where DSRM comes in with a detailed approach to solving the problem, through the design of the architecture and functionality; then the creation and development of the artefact. Once the artefact has been developed, it is then evaluated in stage 4 of DSRM. There is a moment of reflection on the output, which feeds back to development as a way of improving the output. The final stage is the communication of the framework though scholarly platforms and to various audiences.

DSRM was also found appropriate to the problem setup. A business problem was identified and DSR is the right tool to develop and implement a solution to address the problem. The problem was phenomenological hence an artefact was the solution, making DSR the correct choice for a paradigm with a case study strategy.

8.3.2 Scientific reflection

Technological advancements have revolutionised all businesses to be technology-driven. In so doing, end users of technology have been faced with the challenge of having to make decisions which they traditionally regarded as specific to IT practitioners. Among them are security-related decisions which are mostly perceived by end users to be complex. Each program used to accomplish work related tasks has its own set of security features which differ from the next program. As is the nature of technology-centric organisation, the end user has to complete several tasks related to their duties using different end user programs. For instance, one uses a document creator to create a memo, and to ensure its integrity one signs it and shares it electronically using an email client program in PDF format. In this simple case, the end user has interacted with three different programs with different security interactions. User studies have shown that the user remains with a negative experience and usually chooses the easier way of responding to security interactions, which results in security breaches.

Literature has shown that there are no mechanisms in place to measure the user experience of these interactions; hence, there is a need to come up with metrics and methods to address this. The thesis contributes a framework which can be applied to evaluate, influence and maintain

acceptable user experience levels. The framework is positioned to contribute to InfoSec, HCI and EUP design.

8.3.3 Substantive reflection

The study focused on two broad fields namely InfoSec and UX which are both complex and wide. The scope of the study covers Computer Science, Cognitive Psychology, UX and Industry Design. The nature of the fields ensured a broad understanding of human factors affecting end user interaction with security features. This enabled the identification of UX evaluation criteria suitable for InfoSec in particular focusing on EUPSF in MS Word and Adobe. The understanding of the HCI, InfoSec and USec enabled the development of the EUPSFUX evaluation framework.

8.4 LESSONS LEARNT

Self-realisation was the greatest gift I took out of this research journey. As a technical person technology has always been my focus and I believed that if a product is designed with a user goal in mind, then it is automatically usable and the end user accepts and enjoys it. During my journey new realities were presented that altered my personal views of end users. A new passion was awakened and I cannot believe how I ever missed my passion for the user perspective of technology. I developed a deeper understanding of human behaviour, experience and motivation when they interact with technology.

Rich knowledge and appreciation of my fields of study were gained, together with an interdisciplinary appreciation for research. Research passion, skills and abilities were tremendously developed. I learnt to value that the role of the end user is the success of technology implementation and in shaping the organisational security culture.

At the beginning, the aim was to evaluate secure user experience, but as the research problem unfolded it became apparent that there were other aspects of UX that I needed to understand first. Secure UX is not just a matter of marrying information security and user experience fields, but it is a process of understanding the fields holistically and being able to apply the understanding to arising situations. Human factors are very complex and dynamic. These present a challenge in evaluating user experience. In addition, security presents itself to end users in a variety of forms, increasing the complexity of the study.

As a step towards this grand dream, a way of evaluating UX of end user interaction with EUPSF has to be developed. This can later be tailored to evaluate the security of user experience. A new challenge presented itself in the form of end user awareness (EUA). EUA assumed a central position in all efforts to understand security and interaction. As such, it had to be attended to. EUA anchors InfoSec, UB and UX alike, so how then can the security posture, user behaviour and user experience be evaluated without first evaluating the product awareness levels in context? Moreover, UX is an intersection of end user and product (technology) characteristics in a specific context.

A new passion was birthed: EUA of information security factors. This led to the development of EUA metrics using goal-question, bottom-up methods. To understand the security of UX, UB, HCI, security objectives and characteristics, as well as the human nature in organisational setup, have to be investigated fully.

8.5 RESEARCH LIMITATIONS

The research was conducted in only one academic institution; hence, there was no comparison of the outcome and the impact of the organisational culture. The organisational culture was not studied in depth to enable conclusions to be drawn about what drives the human interactions. The study; however, managed to gain a glimpse of the tip of the iceberg of what the people do.

The framework was not empirically validated in the case site to evaluate the actual applicability, as it requires a long period of time, which was beyond the scope of a PhD study. The nature of the research was an intersection of many fields and, as such, it was difficult to find experts with tri-expertise in the fields of InfoSec, UX and HCI. Only one such expert was available. It would have been more interesting to compare the evaluation from multiple sources with similar expertise.

The strength of the framework is that it was developed from a user perspective of end users in a typical case. However, the weakness is that it does not address user behaviour and organisational security culture, as they are beyond the scope of this study.

8.6 FUTURE DIRECTIONS

In future, the framework will be tested in different setups and the domain of the research participants will be broadened to allow for generalisability of the framework. An in-depth culture

study of the case site will be carried out in the quest to understand their underpinning assumptions, which influence both individual and organisation values and behaviour. Finally, further research in secure UX as a research focus will be pursued. Also important is the study of the user behaviour domain of HCI and its influence on organisational information security culture.

8.7 CONCLUDING REMARKS

The main objective of the research work was to develop a framework that would evaluate UX of end user program security features. To achieve this goal, three sub-objectives were formulated and were achieved through several researches aimed at addressing the corresponding research questions as presented in Chapter 1, Section 4. Table 8-1 presents the research questions and answers.

Table 8-1: Research question, answers and evidence

Research question	Answer	Evidence
What are the components of a framework to evaluate UX of end user program security features?	Components and requirements of end user program security features' UX were determined and used to develop the EUPSFUX framework. The identified components are: factors affecting UX (users (people), technology and organisation strategy); UX evaluation criteria; implementation guidelines; UX intervention and stakeholders.	Framework, implementation guidelines and evaluation metrics
What are the factors affecting UX with embedded security features in end user programs?	Identified factors: • Security feature awareness • Policy awareness and implementation • Organisational culture • Feelings evoked by	Theoretical framework, Figure 5-6 Components of EUPSFUX framework Paper 1: Factors affecting user experience with security features Paper 2: Metrics for security

Research question	Answer	Evidence
	interaction • Usability of the security feature • End user's attitudes and perceptions of the security task • Prior user experience • User behaviour with security features	awareness
What are the suitable usable security criteria/ methods that can be used to evaluate UX of end user program security features?	To determine the best USec evaluation methods for evaluating UX of application security features. Develop heuristic evaluation and associated checklists. the identified 17 criteria are: Awareness/expected; Motivating; Comfortable; Useful; Desirable; Accessible; Visible / readily displayed/ findable; Valuable/ impact of use; Usable; Supported; Understandable/complexity/ learnable; Long term experience/ memorability; Security/ safety; Efficient; Effective; Satisfaction; Exciting/perception/ emotion	Heuristic evaluation, framework evaluation criteria
Which UX metrics/ evaluation criteria can be used to determine the UX of end user program security features?	To determine UX criteria that can be adopted for end user programs security features UX (EUPSFUX).	Heuristic evaluation, framework evaluation criteria UX metrics for UX in application program security

The research work mainly followed an interpretivist philosophy employing inductive and design science approaches complemented with case study strategies. Data collection and gathering followed the qualitative method using semi- structured interviews, surveys and heuristic evaluations as instruments.

Findings from the studies were published in peer reviewed conferences and journals in Information Security and Human Computer Interaction. The research papers are partially presented in Chapter 5, where the actual studies are described and the full papers are part of the appendices and are presented in Appendix C1, Appendix C2 and Appendix C3.

A discussion of the framework development process is presented in Chapter 6 and 7 where the framework is developed and evaluated.

The framework brings together the factors that affect users with information security in application programs; metrics for measuring user awareness of security features; user experiences of interaction with security features and their behaviour towards the features within an academic institution.

Making security awareness programs available which focus on awareness, then knowledge and skills, among the staff members of an academic institution would enhance positive security behaviours in the organisation. Consequently, as they interact with students they will impart the information regarding security positive behaviours to them and this will result in overall secure user experiences for all involved. The revised theoretical framework in Figure 6-14 shows how the different elements of HCI influence InfoSec and UX in the study context.

Awareness is the basis of feelings while interacting with technology. The feelings shape the attitudes and perceptions which, in turn, influence user experience with the technology in use. Negative feelings mean that the user will resist using the technology and consequently, there will be no security. On the other hand, positive feelings mean that the users have a good perception of the technology, and a positive experience while interacting. As a result, they behave in a secure manner; hence, they secure their information.

The proposed framework could easily be used by the case site and other similar setups.

REFERENCES

A

Abbasi, M. Q., Lew, P., Rafique, I., & Li, Z. (2012). User Experience Evolution Lifecycle Framework. *International conference on Information, Systems and Engineering (ICISE). 61*, pp. 15-17. Zurich, Switzerland: World Academy of Science, Engineering and Technology . Retrieved May 24, 2012

Abras, C., Maloney-Krichmar, D., & Preece, J. (2005). User-Centered Design. *The Berkshire Encyclopedia of Human-Computer Interaction: When Science Fiction Becomes Science Fact, 2*, 763-768.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise security mechanisma and how to take remedial measures. *ACM, 42*(12), 40-46.

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

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior.* NJ: Prentice Hall.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: A Behaviour Compliance Conceptual framework. In C. Boyd, & W. Susilo (Ed.), *Australasian Information Security Conference (AISC). 105.* Brisbane: Australian Computer Society, Inc. Retrieved from http://eprints.qut.edu.au/29221/1/29221.pdf

Arachchilage, N. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38* , 304–312. doi:10.1016/j.chb.2014.05.046

B

Baecker, R. M., Grudin, J., Buxton, W. A., & Greenberg, S. (1995). *Readings in human computer interaction:Torward the year 2000.* (Second ed.). Los Altos, CA: Morgan Kaufmann Publishers.

Balatbat, C. (2013). *A Beginner's Guide to Heuristic Evaluation pRT 1*. Retrieved from Foolproof Labs' Blog: http://blog.foolprooflabs.com/2013/11/beginners-guide-heuristic-evaluation-part-1/

Balfanz, D. (2004). Toward usable security. *DIMACS Workshop on usable privacy and security software*. New Jersey: Palo Alto Research centre. Retrieved from http://dimacs.rutgers.edu/Workshops/Tools/abstract-balfanz.pdf

Battarbee, K. (2004). *Co-Experience: Understanding User Experiences in Social Interaction (Doctoral dissertation).* Helsinki: University of Art and Design.

Beisse, F. (2004). Chapter 1 ntroduction to end-user computing. In F. Beisse, *A Guide to Computer User Support for Help Desk and Support Specialists* (3rd ed., pp. 1-36). Phoenix: Course Technology. Retrieved August 13, 2013, from http://ghc.edu/faculty/slloyd/CIS211/Chap1.pdf

Bhattacherjee, A. (2012). *Social Science Research:Principles, Methods, and Practices* (2 ed.). Florida: Global Text Project.

Borgatti, S. P. (1999). *Elements of Research*. Retrieved from Analytictech.com: http://www.analytictech.com/mb313/elements.htm

Brotby, K. W., & Hinson, G. (2013). *Brotby, W. Pragmatic security metrics: applying metametrics to information security.* New York: Auerbach Publications. Retrieved from http://common.books24x7.com/toc.aspx?bookid=47301.

C

Campbell, J. (2000). *Usability evaluation*. Retrieved from http://www.usabilityhome.com/: http://www.usabilityhome.com/

Campbell, J. (2011). *The Meaning of User Experience.* User Intelligence. Retrieved 2 12, 2013, from http://www.userintelligence.com/?q=ideas/blog/2011/04/meaning-user-experience

Carroll, J. M. (2014). Human Computer Interaction (HCI)- brief intro. In M. HumaSoegaard, & R. F. Dam, *The Encyclopedia of Human-Computer Interaction* (2nd ed.). Aarhus, Denmark: The Interaction Design Foundation. Retrieved from https://www.interaction-design.org/encyclopedia/human_computer_interaction_hci.html

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. *ARES 2013, SecOnt workshop* (pp. 546–555). Regensburg, Germany: IEEE. Retrieved from http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf

Chia, P., Ruighhaver, A. B., & Maynard, S. B. (2002). Understangind organisational security culture. *PACIS2002*. Japan.

Chin, J. P., Diehl, V. A., & Kent, N. L. (1998). Development of an Instrument Measuring User Satisfaction of the Human-Computer Interface: Interface Evaluations. *ACM CHI'88 Conference on Human Factors in Computing Systems* (pp. 213-218). ACM.

Ciampa, M. (2011). *Security+ Guide to Network Security Fundamentals* (3rd ed.). Boston: Tomson Course Technology. Retrieved 2011

Colabro, G. (2012). *Top 10 Tools to Measure User Experience*. Pragmatic Marketing, Inc. Retrieved march 23, 2012, from http://www.pragmaticmarketing.com/resources/top-10-tools-to-measure-user-experience

Conner, M., & Armitage, C. J. (1998). Extending the theory of planned behavior: A review and avenues for further research. *Journal of Applied Social Psychology, 15*, 1429 -1464.

Cranor, L. F. (2008). A framework for reasonong about the human in the loop. (pp. 1-15). Berkeley: UPSEC'08 proceedings of the 1st Conference on usability, psychology and security.

Cranor, L. F. (2009). Introduction to usable security reasoning about the human in the loop. Cylab Usable Privacy and Security (CUPS).

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: Designing systems people can use.* Cambrige, USA: O'Reilly Media Inc.

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). London: Sage Publications.

Creswell, J. W. (2007). *Quaitative inquiry and research design: Choosing among five approaches* (2nd ed.). Thousand Oaks: Sage Publications.

Crinson, I., & Leontowitsch, M. (2011). *Public Health textbook: Qualitative methods.* UK: PHAST (Public Health Action Support Team CIC). Retrieved August 4, 2012, from http://www.healthknowledge.org.uk/public-health-textbook/research-methods/1d-qualitative-methods

D

Danino, N. (2001). *Heuristic Evaluation – a Step By Step Guide Article*. Retrieved from sitepoint.com: http://www.sitepoint.com/heuristic-evaluation-guide/

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13* (3), 319-340.

Denzin, N. K., & Lincoln, Y. S. (2005). *The sage handbook of qualitative research* (3rd ed.). Thousand Oaks: Sage Publications.

DePaulo, P. (2000). Sample size for qualitative research. *QUIRKS*, 12. Retrieved August 8, 2012, from http://www.quirks.com/articles/a2000/20001202.aspx?searchID=496600809

Desmet, P., & Hekkert, P. (2007). Framework of product experience. *International journal of design, 1*(1), 57-66.

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework for linking culture and improvement initiatives in organizations. *Academy of Management Review*, *25*(4), 850-863.

Dey, I. (2005). *Qualitative data analysis: A user-friendly guide for social scientists.* . London: Taylor & Francis e-Library. doi: ISBN 0-203-72073-3

Dooley, L. M. (2002). Case study research and theory building. *Advances in Developing Human Resources, 4*(3), 335-354.

E

Edwards, K. W., Poole, S. E., & Stoll, J. (2008). Security Automation Considered Harmful? *NSPW '07 Proceedings of the 2007 Workshop on New Security Paradigms* (pp. 33-42). New York: ACM.

Eisenhart, M. (1991). What are the types of research frameworks? Retrieved 2014, from http://e-library.math4teaching.com/what-are-the-types-of-research-frameworks/

Ellis, T. J., & Levy, Y. (2008). Framework of Problem-based Research: A Guide for Novice Researchers on the Development of a Research-Worthy Problem. *Informing Science: the International Journal of an Emerging Trans-discipline, 11*, 17-33. Retrieved August 17, 2013, from http://www.inform.nu/Articles/Vol11/ISJv11p017-033Ellis486.pdf

F

Faulkener, X. (2000). *Usability Engineering.* Macmillan Press Ltd.

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

Forlizzi, J., & Battarbee, K. (2004). Understanding Experience in Interactive Systems. *DIS2004. 787*, pp. 261-268. Cambridge: ACM. doi:ACM 1-58113-787-7/04/0008

Forlizzi, J., & Ford, S. (2000). The building blocks of experience:an early framework for interaction designers. *DIS '00 3rd conference on Designing interactive systems: processes, practices, methods, and techniques (pp. 419* (pp. 419-423). Brooklyn, New York.: ACM. doi:10.1145/347642.347800

Furnell, S. (2004). Using security: easier said than done? *Computer Fraud & Security*, 6-10.

Furnell, S. (2005). Why users cannot use security. *Computers and Security, 24*(4), 274-279.

Furnell, S. (2006). *Usability Challenge- Can End-users Use Security?* Information Security.

Furnell, S. (2010). Usability versus complexity - striking the balance in end-user security. *Network Security, 2010*(12), 13-17. doi:10.1016/s1353-4848 (10) 70147-1

Furnell, S. M., Jusoh, A., & Katsabas, D. (2005). The Challenges of understanding and using security: A survey of end-users. *Computers and Security, 25*, 27-35. Retrieved January 24, 2012, from www.elsevier.com/locate/cose

G

Garfinkel, S. L. (2005). *Design principles and patterns for computer systems that are simulteneously usable and secure.* MA: MIT.

Garrett, J. J. (2009). *state of ux design*. Retrieved December 2, 2013, from uxdesign.com: http://uxdesign.com/events/article/state-of-ux-design-garrett/203#sthash.VNVjpDz7.dpuf

Garrett, J. J. (2011). *The elements of user experience: User-cntered design for the web and beyond* (2nd ed.). Berkeley: New Riders.

Government of Namibia. (2012). *Namibia's Fourth National Development Plan (NDP_4).* Windhoek: Government of the republic of Namibia. Retrieved from npc.gov.na/ndp4

H

Hassenzahl, M. (2004). The thing and I:understanding the relationship between user and product. In *Funology* (Vol. 25, pp. 31-42). Norwell, MA, USA: Kluwer Academic Publishers. doi:10.1080/01449290500330331

Hassenzahl, M., & Tractinsky, N. (2006). User experience - a research agenda. *Behaviour & Information Technology, 25*(2), 91-97. doi:10.1080/01449290500330331

Hayden, L. (2010). *IT security metrics: A practical framework for measuring security and protecting data.* USA: McGraw-Hill.

HCISecAdmin. (2009). *Human-Computer Interaction Security (HCISec).* Retrieved from Human-Computer Interaction Security (HCISec): http://hcisec.blogspot.com

Herley, C. (2009). So Long, And No Thanks for the Externalities:The Rational Rejection of Security Advice by Users. *NSPW 09* (pp. 133-144). OXford: ACM. doi:978-1-60558-845-2/09/09

Hertzum, M., Jørgensen, N., & Nørgaard, M. (2004). Usable Security and E-Banking: Ease of Use vis-à-vis Security. *Australasian Journal of Information Systems,, 11*(special issue (2004)), 52-65.

Hertzum, M., Juul, N. C., Jørgensen, N., & Nørgaard, M. (2004). Usable Security and E-Banking: Ease of Use vis-à-vis Security. *OZCHI 2004* . Wollongong, Australia: University of Wollongong. Retrieved from http://akira.ruc.dk/~nielsj/research/publications/eBanking-ozchi.pdf

Herzog, A., & Shahmehri, N. (2007). User Help Techniques for usable security. *ACM*(1-59593-635-6/07/0003).

Hevner, A. R., Ram, S., March, S. T., & Park, J. (2004). Design Science in Information Systems research. *MIS Quarterly, 28*(1), 75-105.

Hevner, A. R. (2007). A three-cycle view of design science research. *Scandinavian Journal of Information Systems, 19*(2), 87-92.

Hewett, T. T., Baecker, R., Card, S., Carey, T., Garsen, J., Mantei, M., . . . Verplank, W. (1992). *ACM SIGCHI Curricula for Human-Computer Interaction.* Broadway, New York: ACM Inc.

Hewlett Packard. (2011). *Top Cybe rSecurity Risks Report.* Hewlett Packard Development Company, L.P. Retrieved from http://www.hpenterprisesecurity.com/collateral/report/2011FullYearCyberSecurityRisksReport.pdf

I

International Organization for Standardization/International Electrotechnical Commission. (1999). ISO 13407:1999, Human-Centered Design Processes. Geneva.

Isaacs, S. (2007). *ICT in Education in Namibia.* Windhoek: www.infodev.org.

ISACA. (2009). *introduction to the business model for information security.* Rolling Meadows, IL: ISACA. Retrieved from http://www.isaca.org/knowledge-center/research/documents/introduction-to-the-business-model-for-information-security_res_eng_0109.pdf

ISO 9241-11. (1998). *Ergonomic requirements for office work with visual display terminals (VDTs) Part 11: Guidance on Usability.* ISO.

ISO 9241-210. (2010). Ergonomics of Human System Interaction- Part 210, Human-Centred design for Interactive Systems. Retrieved September 28, 2012, from http://www.allaboutux.org/ux-definitions

ISO/IEC. (1999). ISO/IEC 12207, Information Technology, Software Life Cycle Processes. Geneva.

ISO/IEC 9126. (2001). *ISO/IEC 9126-1 (2001). International Standard. Information technology – Software product evaluation- quality characteristics and guidelines for their use.* Geneva, Switzerland: International Organization for Standardisation. Retrieved March 20, 2011, from http://webstore.iec.ch/preview/info_isoiec9126-1%7Bed1.0%7Den.pdf

ISO/IEC 9126-1. (2001). International Standard. Information technology – Software product evaluation- quality characteristics and guidelines for their use. *ISO/IEC 9126-1*. Geneva, Switzerland: International Organization for Standardisation. Retrieved March 20, 2011, from http://webstore.iec.ch/preview/info_isoiec9126-1%7Bed1.0%7Den.pdf

J

Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods (IJQM), 8*(4), 49-62.

Jetter, H.-C., & Gerken, J. (2006). A simplifiedmodel of user experience for practical application. *the 2nd internatioanl Open Workshop, Userexperience torwards a unified view* (pp. 106-1111). Oslo, Norway: NordiHCI.

Jetter, H.-C., & Gerken, J. (2007). A simplified model of user experience for practical application. *NordiCHI 2006. The 2nd COST294-MAUSE International Open Workshop User eXperience- Torwards a unified view*, pp. 106-111. Oslo: ACM.

Johnson, M. E., & Goetz, E. (2007). Embedding Information Security into the Organization. *IEEE Security & Privacy, 5*(3), 16-24. doi:10.1109/MSP.2007.59

Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human coputer interfaces. *Computers & Security, 22*(8), 675-684.

Joo, L. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the Relationship between OrganizationalCulture and Information Security Culture. *7th Australian Information Security Management Conference* (pp. 88-97). Perth: Edith Cowan University Research Online.

K

Kainda , R., Flechais, I., & Roscoe, W. A. (2010). Security and Usability:analysis and evaluation. 1-8.

Kaiser, J., & Reichenbach, M. (2002). Evaluating security tools towards usable security: A usability taxonomy for the evaluation of security tools based on a categorization of user errors. *The IFIP 17th World Computer Congress - TC13* (pp. 1-10). CiteSeerX. Retrieved March 23, 2013, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.12.7527&rep=rep1&type=pdf

Katsabas, D., Furnell, S. M., & Dowland, P. S. (2005). Using Human Computer Interaction principles to promote usable security. *Fifth International Network Conference (INC 2005)*, (pp. 235 - 242). Samos, Greece.

Keinonen, T. (1998). Usability of Interactive Products. In T. Keinonen, *One-dimensional usability - influence of usability on consumers' product preference* (p. website). Helsinki: UIAH publication. Retrieved from UIAH: http://www2.uiah.fi/projects/metodi/printabl/158.htm

Keinonen, T. (2007). One-dimensional usability influence of usability on consumers' product preference. UIAH.

Klemmer, S. (2012). *Introduction to Human-Computer Interaction Design.* Retrieved January 2013, from http://openclassroom.stanford.edu/MainFolder/courses/HCI/CS147Icon.jpg

Krieger, P. (2009). privacy policies and usability. *Third European Privacy Open Space* (pp. 81-84). Europahaus in Vienna: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Retrieved from https://www.datenschutzzentrum.de/download/225044-D15-Report-PrivacyOS-Conference-Vienna-2009.pdf

Kuniavsky , M. (2010). *Smart Things: Ubiquitous Computing User Experience Design* (1st ed.). Burlington: Morgan Kaufmann, Elsevier.

L

Law, E. L.-C., Roto, V., Hassenzahl, M., Vermeeren, A. P., & Kort, J. (2009). Understanding, scoping and defining user experience a survey approach. *27th international conference on Human factors in computing system, CHI'09* (pp. 719-728). Boston, MA: ACM.

Lester, F. K. (2005). On the theoreticall, conceptualand philosophical foundations froresearch in mathematics education. *ZDM, 37*(6), 457-467.

Lethbridge, T. C., & Laganiere, R. (2005). *Object-Oriented Software Engineering:Practical Software Development using UML and Java* (2nd ed.). London: McGraw Hill. Retrieved 2013, from http://fit.hcmup.edu.vn/~haits/English%20Courses/Technical%20Software%20Development/__Object_Oriented_Software_Engineering__Practical_Software_Development_using_UML_and_Java.pdf

Letts, L., Wilkins, S., Law, M., Stewart, D., Bosch, J., & Westmorland, M. (2007). Guidelines for Critical Review Form:Qualitative Studies (Version 2.0).

Lew, P., Olsina, L., & Zhang, L. (2010). Integrating Quality, Quality in Use, Actual Usability and User Experience. *6th Central and Eastern European Software engineering Conference CEESECR* (pp. 117-123). Moscow, Russia: IEEE.

Lewis, J. R. (1995). IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use. *International Journal of Human-Computer Interaction, 7*(1), 57-78.

Lin, H. X., Choong, Y.-Y., & Salvendy, G. (1997). A Proposed Index of Usability: A Method for Comparing the Relative Usability of Different Software Systems Usability Evaluation Methods . *Behaviour and Information Technology, 16*(4/5), 267-278.

Long, L. A. (2012). *Profiling Hackers.* The SANS Institute. Retrieved December 6, 2012, from http://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864

Lowgren, J. (2014). Interaction Design- brief intro. In M. a. Soegaard, *The Encyclopedia of Human-Computer Interaction* (2nd ed.). Aarhus, Denmark: The Interaction Design Foundation. Retrieved from https://www.interaction-design.org/encyclopedia/interaction_design.html

Lund, A. M. (2008, September 05). *Measuring Usability with the USE Questionnaire*. Retrieved from HCI Bibliography: http://hcibib.org/bs.cgi?searchtype=question&query=U.Lund.2001

Lyne, J. (2014). *Security threat trends 2015: Predicting what cyber security will do in 2015 and beyond.* Oxford: Sophos. Retrieved from https://www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf

M

Mahlke, S. (2008). *User experience of interaction with technical systems: theories, methods, empirical results, and their application to the development of interactive systems.* Berlin: Technical University of Berlin. Retrieved July 28, 2013

March, S. T., & Smith, G. F. (1995, December). Design and Natural Science Research on Information Technology. *Decision Support systems, 15*(4), 251-266.

Mason, M. (2010). Sample size and saturation in PhD studies using quantitative interview.s. *Qualitative Social Research, 11*(3). Retrieved from http://nbn-resolving.de/urn:nbn:de:0114-fqs100387

Mathiasen, N. R., & Bodker, S. (2008). Threats or threads: from usable security to secure experience? *NordiCHI'08. 5*, pp. 283-289. New york: ACM. doi:10.1145/1462160.1463191

Mead, N. R., Allen, J. H., Ardis, M., Hilburn, T. B., Kornecki, A. J., Linger, R., & McDonald, J. (2010). *Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum.* Software Engineering Institute. Hanscom: Carnegie Mellon University. Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_78257.pdf

Meyers, A. B., & Sylveste, B. A. (2006, February). The Role of Qualitative Research Methods in Evidence-Based Practice. *NASP Communiqué, 34*(5). Retrieved July 7, 2015, from http://www.nasponline.org/publications/cq/cq345research.aspx

Microsoft. (2013). Protection settings for Office 2013. USA: Microsoft. Retrieved from http://technet.microsoft.com/en-us/library/dn166707%28v=office.15%29.aspx

Miles, M. B., & Huberman, M. A. (1994). *Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed.). Thousand Oaks: Sage Publications.

Milligan, K. (2006). *Using Information and Technology in the workplace.* Australia: Australian Research Alliance for Children and Youth.

Minge, M. (2008). Dynamics of User Experience. *Workshop on research goals and strategies for studying User Experience and Emotion at NordiCHI 2008* (pp. 429- 452). Lund, Sweden: NordiCHI 2008.

Morville , P. (2004, June 21). *User experience Design*. Retrieved March 7, 2012, from semanticstudios.com: http://semanticstudios.com/publications/semantics/000029.php

Muller, G. (2006). The present and the future of usable security. Retrieved from http://ec.europa.eu/information_society/istevent/2006/cf/document.cfm?doc_id=1954

Myers, M. D., & Avison, D. E. (2002). *Qualitative Research in Information Systems: A Reader.* London: Sage.

N

Nalzaro, L. M. (2012, June 9). Theoretical and conceptual framework. Technology. Retrieved from http://www.slideshare.net/ludymae/chapter-6theoretical-conceptual-framework

Nielsen , J. (1993). *Usability Engineering.* . San Francisco, CA, USA : Morgan Kaufmann Publishers Inc.

Nielsen, J. (1994). Heuristic evaluation. In J. Nielsen, & R. L. Mack, *Usability inspection methods.* New York: John Wiley & Sons.

Nielsen, J. (1995, January 1). *How to Conduct a Heuristic Evaluation*. (J. Nielsen, D. Norman, & B. Tognazzini, Editors) Retrieved May 8, 2012, from Nielsen Norman group: http://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/

Nielsen, J. (1995). Usability Inspection Methods. *CHI 95* (pp. 377-378). Colorado: ACM. Retrieved from http://www.sigchi.org/chi95/proceedings/tutors/jn_bdy.htm

Nielsen, J. (2000, November 26). *Security & Human Factors*. Retrieved from Nielsen Norman Group: http://www.nngroup.com/articles/security-and-human-factors/

NRCNA. (2010). *" 5 Overarching Challenges to Advancing Research in Usability, Security, and Privacy ." Toward Better Usability, Security, and Privacy of Information Technology.* NATIONAL RESEARCH COUNCILOF THE NATIONAL ACADEMIES. Washington, DC: The National Academies Press.

Nurse, J. R., Creese, S., Goldsmith, M., & Lamberts, K. (2011, September). Guidelines for usable cybersecurity:Past and Present. *Cyberspace Safety and Security (CSS), 3*, pp. 21-26. Retrieved from http://www.teaseproject.info/publications/CSS2011_NCGL_authors_final.pdf

O

Oates, B. J. (2012). *Researching Information Systems and Computing* (2nd ed.). London: Sage Publications.

P

Paditar, J. (2014). Developing a conceptual framework. Gujarat: Education. Retrieved from http://www.slideshare.net/drjayeshpatidar/ppt-developing-a-conceptual-framework

Pajares, F. (2007). *The elements of a proposal*. Retrieved from Emory University: http://www.uky.edu/~eushe2/Pajares/proposal.html, http://des.emory.edu/mfp/proposal.html

Patton, M. (1990). Designing Qualitative Studies. In *Qualitative evaluation and research methods* (pp. 169-186). Beverly Hills, CA: Sage. Retrieved from http://legacy.oise.utoronto.ca/research/field-centres/ross/ctl1014/Patton1990.pdf

Payne, S. C. (2006). *A Guide to Security Metrics: SANS Security Essentials GSEC Practical Assignment Version 1.2e (2007).* SANS.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee , S. (2008). A design Science Research Methodology for Information Systems research. *Journal of Management Information Systems, 24*(3), 47-77.

Perlman, G. (1997). Practical Usability Evaluation. *CHI 97 Electronic Publications: Tutorials.* CHI 97 Electronic Publications. Retrieved from http://www.sigchi.org/chi97/proceedings/tutorial/gp.htm or http://garyperlman.com/quest/quest.cgi?form=USE

Pfleeger, C. P., & Pfleeger, L. S. (2007). *Security in Computing* (4th ed.). New Jersey, USA: Pearson Education Inc.

Prat, N., Comyn-Wattiau, I., & Akoka, J. (2014). Artifact evaluation in Information Systems design science research- A holistic view. *The 18th Pacific Asia Conference on Information Systems (PACIS 2014).* Chengdu, China: PACIS. Retrieved from http://cedric.cnam.fr/fichiers/art_3208.pdf

Preece, J. (2002). *Interaction Design: Beyond Human Computer Interaction.*

R

Ravdev, S., & Johnson, G. (1989). *Evaluating usability in human computer interfaces: a practical method.* Chichester, UK: Ellis Horwood Limited.

Ross, J. A. (2008). *Security Engineering: A guide to building dependable distributed systems* (2nd ed.). Cambridge: John Wiley & Sons.

Rosson, M. B., & Carroll, J. M. (2002). Scenario-Based Design. In J. J. Sears, & J. J. Sears (Ed.), *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications.* (pp. 1032-1050). NJ,USA: Lawrence Erlbaum Associates. Retrieved from http://ocw.tudelft.nl/fileadmin/ocw/courses/IntelligentUserExperienceEngineering/res00110/2_RossonCarrollSBDforHandbook2002.pdf

Roto, V. (2007). User Experience from product creation perspective. In E. Law, A. Vermeeren, M. Hassenzahl, & M. Blythe, *Towards the evaluation of User Experience* (pp. 31 - 34). Lancaster.

Roto, V., Vermeeren, A., Law, E. L.-C., & Hoonhout, J. (2011). *UX-WhitePaper Bringing clarity to the concept of user experience.* white paper, Dagstuhl . Retrieved December 6, 2012, from http://www.allaboutux.org/files/UX-WhitePaper.pdf

Roto, V., Vermeeren, A., Law, E. L.-C., Lee, M., Pihkala, K., Castro, B., . . . Obrist, M. (2010). User experience evaluation methods: current state and development needs. (pp. 521-530). Reykjavik: NordiCHI2010. Retrieved from All About UX : http://www.allaboutux.org/

Roto, V., Vermeeren, A., Law, E. L.-C., Lee, M., Pihkala, K., Castro, B., . . . Obrist, M. (2012, December 7). *All About UX* . Retrieved from All About UX : http://www.allaboutux.org/

Rubin , J., & Chisnell , D. (2008). *Handbook of UsabilityTesting: How to Plan, Design, and Conduct EffectiveTests* (2nd ed.). Indianapolis: John Wiley & Sons.

Ryan, G. W., & Bernard, R. H. (2000). Data Management and Analysis Methods. In N. K. Denzin, & Y. S. Lincoln, *Handbook of Qualitative Research,* (pp. 769-802). London: Sage Publication.

S

Saffer, D. S. (2010). *Designing for interaction. Second Edition.* Berkeley, CA: New Riders.

Saint- Germain, R. (2005). Information security management best practices based on ISO/IEC 17799. *The Information Management Journal*, 60-66.

SANS. (2009, September). *The Top Cyber Security Risks*. Retrieved from SANS.org: https://www.sans.org/The Top Cyber Security Risks.htm#trends

SANS. (2011). *Security prediction 2012 & 2013 The emerging security threat.* SANS. Retrieved February 24, 2012, from http://www.sans.edu/research/security-laboratory/article/security-predict2011

Sasse, A. M. (2003). Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery. *Workshop on Human-Computer Interaction and Security Systems at CHI 2003.* Floria: URCL. Retrieved from http://www.andrewpatrick.ca/CHI2003/HCISEC/hcisec-workshop-sasse.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th ed.). England: Pearson Education Limited.

Sauro, J., & Kindlund, E. (2005). A method to standardize usability metrics into a single score. *Human Factors in Computing Systems (CHI 2005)* (pp. 401-409). Portland, Oregon, USA: ACM. doi:1-58113-998-5/05/0004

Sauro, J., & Lewis, J. R. (2012). *Quantifying user experience: Practical ststistics for user research.* Massachusetts: Morgan Kaufmann.

Schein, E. H. (2004). *Organizational culture and leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.

Schreier, M. (2012). *Qualitative Content Analysis in Practice.* Sage Publications Ltd.

Schulze, K., & Krömker, H. (2010). A Framework to Measure User Experience of Interactive Online Products. *7th International Conference on Methods and Techniques in Behavioral Research* (pp. 261-264). Eindhoven, Netherlands: ACM.

Sekaran, U., & Bougie, R. (2009). *Research methods for business: A skill Building Approach.* (5th ed.). UK: John Wiley & Sons.

Shackleford, D. (2011). *Security of applications: It takes a village.* The SANS Institute.

Sharma, A. (2013). Do We Really Need Traditional Usability Lab for UX Practice? In A. Sharma , A. Chakrabarti, & R. V. Prakash (Eds.), *ICoRD'13: Global Product Development* (pp. 399-409). India: Springer India.

Shields, P. M., & Rangarajan, N. (2013). *A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management.* Stillwater: New Forums Press.

Shneiderman, B., & Plaisant, C. (2005). *DESIGNING THE USER INTERFACE* (4th ed.). London: Pearson Education Inc.

Shrestha, A., Cater-Steel, A., & Toleman, M. (2014). How to communicate evaluation work in Design Science Research? an exemplar case study. *25th Australasian Conference on information sysytems.* Auckland, New Zealand: ACIS. Retrieved August 10, 2015, from http://eprints.usq.edu.au/26627/1/Shrestha_Cater-Steel_Toleman_ACIS_2014_PV.pdf

Sieger, H., Kirschnick, N., & Möller, S. (2011). Poster: Towards a user behavior model . Symposium on Usability, Privacy, and Security (SOUPS) 2010.

Simon, H. A. (1996). *The sciences of the artificial* (3rd ed.). Cambridge: Massachusetts Institute of Technology (MIT) Press.

Siponen, M. T. (2000). Critical analysis of different approaches to minimizing user related faults in information systems security: implications for research and practice. *Information management and Computer Security*, *8*, pp. 197-210.

Spears, J. L., & Bark. , H. (2010). User Participation in IS Security Risk Management. *MIS Quarterly, 34*(3), 503-522. Retrieved from http://www.misq.org

Spitzner, L. (2012). *Security awareness maturity model promoting change.* SANS. Retrieved from http://www.securingthehuman.org/blog/2012/05/29/security-awareness-maturity-model-promoting-change#

Spitzner, L.. (2012). *Next generation security awareness programs: securing the human.* SANS. Retrieved from www.securingthehuman.org/blog

Stalling, W., & Brown, L. (2008). *Computer Security Principles and Practice.* Upper Saddle River, NJ: Pearson Prentice Hall.

Statistics, Internet World. (2011). Internet statistics usage : the Big picture. Inrernet WorldStats. Retrieved January 24, 2012, from http://www.internetworldstats.com/stats.htm

Sutcliffe, A. (2009). Designing for User Engagement: Aesthetic and Attractive User Interfaces. *All about UX, Morgan & Claypool Publishers*. (V. Roto, M. Lee, K. Pihkala, B. Castro, A. Vermeeren, E. Law, . . . M. Obrist, Eds.) doi:10.2200/S00210ED1V01Y200910HCI005

Sutcliffe, A., & Hart, J. (2011). Evaluating user experience. Manchester: University of Manchester. Retrieved from http://www.slideshare.net/NorthernUX/evaluating-user-experience

T

Tariq, A. R. (2015). *A brief history of user experience*. Retrieved August 12, 2015, from Invisionapp.com: http://blog.invisionapp.com/a-brief-history-of-user-experience/

Thomson, K.-L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security, 2006*(5), 11-15. doi: doi:10.1016/S1361-3723(06)70356-6

TippingPoint. (2009, September). *The Top Cyber Security Risks*. Retrieved from TippingPoint: https://www.dunkel.de/pdf/200909_TopCyberSecurityRisks.pdf

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook* (6th ed.). CRC Press.

Tomhave, B. L. (2005). *Alphabet Soup: Making Sense of Models,Frameworks, and Methodologies.* http://secureconsulting.net/papers-publications.html.

U

Usability.gov. (n.d.). *User-Centered Design Basics*. Retrieved from usability.gov: http://www.usability.gov/what-and-why/user-centered-design.html

Usabilityhome.com. (n.d.). *Usability Evaluation* . Retrieved from Usabilityhome.com: http://www.usabilityhome.com/

V

Vacca, J. R. (2009). Chapter 1 - Building a Secure Organization. In J. R. Vacca, *Computer and Information Security Handbook:*. Morgan Kaufmann Publishers. Retrieved from Books24

Vaishnavi, V. K., & Kuechler, W. (2008). *Design science research methods and patterns: Innovating Infprmation and Communication Technology*. New York: Auerbach Publication, Taylor Francis Group.

Vaishnavi, V., & Kuechler, W. (2004). *Design Science Research in Information Systems.* Association for Information Systems. Retrieved from URL: http://www.desrist.org/design-research-in-information-systems/

Vaughan, R. (2008). Conceptual Framework.

Venable, J. (2011). Incorporating Design Science Research and Critical Research Into an introductory Business Research Methods Course. *The Electronic Journal of Business Research Methods (EJBRM), 9*(2), 119-129. Retrieved from www.ejbrm.com/issue/download.html?idArticle=261

von Roessing, R. M. (2010). *The Business Model for Information Security*. Rolling Meadows, IL: ISACA. Retrieved from http://www.emi-tuv.hu/uploads/images/133715505073288047021 9/isaca-bmis-2010.pdf

von Solms, B. (2000). Information security - The third wave? *Computers & Security, 19*(7), 615-620.

W

W3Schools. (n.d.). *Browser Statistics*. Retrieved October 4, 2012, from W3Schools.com: http://www.w3schools.com/browsers/browsers_stats.asp

Walshman, G. (1995). interpretive case studies in IS research: nature and method. *Europian Journal of Information Systems*, 74-81. Retrieved from www.palgrave-journals.com/ejis/journal/v4/n2/pdf/ejis19959a.pdf

Weber, R. (2009). Research on ICT for Development: Some reflections on rhetoric, rigor, realityand relevance. *International IDIA Development Informatics Conference.* Kruger National Park: IDIA.

Webster, M. (2015). Merriam-Webster Dictionary. Retrieved from http://www.merriam-webster.com/dictionary/knowledge

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication token. *Computer & Security, 28*, 47-62.

Whitman, M. E., & Mattord, H. (2009). *Principles of Information Security.* USA: Thomson Course technology.

Whitman, M. E., & Mattord, H. (2011). *Principles of Information Security.* USA: Thomson Course technology.

Whitten, A., & Tygar, J. D. (2003). Safe staging forcomputer security. *Workshop on Human-Computer Interaction and Security Systems.* Retrieved from http://www.andrewpatrick.ca/CHI2003/

Whitten, A., & Tygar, J. D. (2005). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In L. Cranor, & G. Simson , *Security and usability: Designing secure systems that People can use* (pp. 679-702). O' Reilly.

Wool, A. (2004). The use and usability of direction based filtering in firewalls. *Computers & Security*, *23*(6), 459- 468.

Wright, P., Wallace , J., & McCarthy, J. (2008). Aesthetics and Experience-centred design. *ACM transactions onComputer- Human Interaction, 15*(4), 1-12. doi:10.1145/1460355.1460360

Y

Yee, K.P. (2002). User interaction design for secure systems. *ICICS' 02 4th international conference on Information and Communications Security* (pp. 278-290). Singapore: Springer-Verlag London,.

Yeratziotis, A., Van Greunen, D., & Pottas, D. (2011). Recommendations for usable security in online health socialnetworks. *IEEE, 15. Yeratziotis, A., van Greunen, D., & Pottas, D. (2011). Recommendations for Usa978-1-4577-0208-2/11* , 220-226.

Yin, R. K. (2009). *Case study Research : Design and Methodds* (4th ed., Vol. 5). London, UK: SAGE Inc.

Z

Zhang, P., & Li, N. (2004). Loveat first sight or sustained effect? the role of perceived quality o user's cognitive reactions to information technology. *ICIS* (pp. 283-295). proc of twenty-fifth ICIS.

Zhang, Z., Basili, V., & Scheiderman, B. (1998). An empirical study of perspective-based usability inspection. *Human Factors and Ergonomics Soceity 42nd Annual Meeting*, (pp. 1346-1350). Chicago.

Zhang, Z., Basili, V., & Shneiderman, B. (1998). Perspective-based usability inspection. *Usability Professionals' Association Conference*, (pp. 281-282). Washington DC.

Zimmermann, P. G. (2008). *Beyond Usability - Measuring Elements of User Experience*. Carcinogenesis. doi:eth 17901

Zurko, M. E. (2005). User-Centered Security: Stepping Up to the Grand Challenge. *Computer Security Applications Conference, 21st Annual. 2005*, pp. 187-200. Tucson, AZ : IEEE. doi:10.1109/CSAC.2005.60

Zurko, M. E., & Simon, R. T. (1996). User-centered security. *Proceedings of the 1996 New Security Paradigms Workshop*, 27-33. Lake Arrowhead, California: ACM.

APPENDIX A1: ONLINE SURVEY QUESTIONNAIRE

End User Information Security Survey

1. Introduction

This questionnaire will be used to address end user issues in Information security focusing on end user application programs. The aim is conduct a pilot study to establish security problems resulting from inadequate support for end users in using security features embedded in application programs they use daily. We will collect data about security awareness, experience with security interaction, usage and problems associated with the use or lack of Application security. The results will be confidential and will only be used to assess the extent of a need to improve the end user's interaction with security features on their computers.
In the first section you will be asked about your general information.

1. Which school/Department are you in? *

2. What is your gender? *

Female Male

3. How long have you been in the Organisation? *

0- 6 Months 6-12 Months 1 Year + 2 Years + 3 Years + 4 Years + 5 Years +

4. What is your age? *

2. User Information Security Awareness

In this section you will answer general question about security threats and intervention strategies.

1.

Have you ever heard of the following? (tick all that apply) :

*

☐ Hacking ☐ Phishing ☐ Spam ☐ Spyware ☐ Virus ☐ Worm ☐ Social Engineering

2. Have you ever been a victim of:

	Yes	No	Don't Know
Hacking	○	○	○
Phishing	○	○	○
Spam	○	○	○
Spyware	○	○	○
Virus	○	○	○
Worm	○	○	○
Social Engineering	○	○	○

3. If any of the answers to 2 is yes, please explain how it happened? *

4.

What are possible sources of information threats? (Tick all the appropriate choices)

*

☐ Internet ☐ USB sticks/ flash ☐ Opening attachments ☐ Opening email from ☐ CDs/DVDs

and external drives		strangers

5. How frequent do you use the following security technologies? *

	Not at all	Rarely	Sometimes	Often	Always
Antivirus	○	○	○	○	○
Firewall	○	○	○	○	○
Antimalware	○	○	○	○	○
Intrusion Detection System	○	○	○	○	○
Passwords	○	○	○	○	○
Patches	○	○	○	○	○
Updates	○	○	○	○	○
Backup	○	○	○	○	○
Encryption	○	○	○	○	○

6.

Do you have any of the above security systems installed on your machine?

*

○ Yes

○ No

○ Don't Know

3. User Behaviour/ Interaction with the programs

You will respond to questions on your interaction with the application programs as you work.

1. How often do you update your Programs? *

Not at all Sometimes When prompted Often Always

2. How do you update? *

Manually Automatically Not at all

3. Do you disable antivirus software/ personal firewalls running on your PC? *

Yes No

4. Do you disable alerts from displaying? *

Yes No

5. What do you think is the reason for programs to display alerts to you? *

6. Do you allow your browser to install add-ons such as Java script, Flash, Active X on your computer? *

Yes No

7. While you are browsing the internet you get a Websense message telling you that the site you are trying to visit is blocked by your organisation. What action do you take? *

8. Do you think it is appropriate for an Organisation to block sites for end users? *

Yes No

9. Are you able to install programs on your computer? *

Yes No

10. Do you download and install free software of choice from the internet? *

Yes No

11. When you connect to the Internet do you always use secure connection? *

Yes No

12. Do you share files with colleagues or students? *

Yes No

13. Which of the following do you use to share your files? (tick all the applicable) *

Memory Stick Network Common Server Email Dropbox GoogleDocs

14. Are you part of any of the following social or professional networks? *

	Yes	No
LinkedIn		
Facebook		
Twitter		

15. What Information do you share with your professional and social networks? *

4. Security and security policy awareness

In this section you will be asked question about your security and security policy awareness. A security policy is a set of goals and rules for an organisation's computer systems usage that ensures security of organisational information and computer assets.

1. Do you receive training on computer security from the technical department? *

Yes No

2. Are you aware of any computer security policies in the Organisation? *

Yes No

3.

To what extent do you know these policies? (1 is not at all and 5 is very well)

*

	1	2	3	4	5
Password					
Wireless					

General Computer usage					
Internet					

5. Do you know and follow the requirements of the policies? *

Yes No

5. Application Program Usage

This section will ask you about the application programs you are using on your computer.

1. To what extent do you use the following programs? *

	Always	Sometimes	Not at all
Word Processors			
Spreadsheets			
Presentation			
Graphics			
Project Management			
Document Readers			
Database Management			
Email			
Web Browsers			
ITS			
Other			

2. Have you ever configured your program security options? *

Yes No

3.

Which one of the following security features in your programs have you used to protect your information?

*

6. User Experience with Program security features.

In this section you will be asked about your experience with program security features and how you feel about the interaction.

1. Have you ever received program notifications warning you to protect your information?
*

Yes No

2. How do you respond to program notifications?/
*

Ignore Read through and make a choice Click anything to get rid of the message

3. Updates prompt you with a notification to install every 3 hours if the expiry date is more than 24 hours away, and hourly if within 24 hours. How do you feel about this? *

4. When you agree to update you get three progress statuses, preparing to download, downloading and installing. Is this helpful? *

Strongly Disagree | Disagree | Not sure | Agree | Strongly Agree

5.

How do you feel when security messages are displayed and require your action? (please tick all the applicable)

*

Irritated | Annoyed | Frustrated | Indifferent | My work is disturbed | It is my responsibility | It is the technician's responsibility

6. Why do you get the feeling you mentioned in the previous question? *

7. Password Usage and Management

In this section you will be asked about your password usage and management.

1. Do you use different passwords for loging to different application programs and websites? *

- Yes
- No
- Sometimes (elaborate)

2. Do you write them down?

- Yes
- No

3. If yes do you protect the password file? *

- Not Applicable
- No
- Yes
- How do you protect it

4. Do you share passwords with colleagues? *

- Yes
- No

5. Do you use the remember password option? *

- Yes
- No

8. Email usage and computer support

You will be asked about the Email programs you use and support you get while using the computer.

1. Does your email filter spam? (put them in junk/ bulk email folder) *

Yes No

2. Do you open emails from unfamiliar names? *

Yes No

3. Do you open all attachments? *

Yes No

4. Do you encrypt your emails before sending them out? *

Yes No

5. Which email client do you use? *

- [ ] Communigate
- [ ] MS Outlook
- [ ] Outlook Express
- [ ] Thunderbird
- [ ] Yahoo mail
- [ ] Gmail

☐ Hotmail

☐ Other (Please Specify)

6.

If your program misbehaves where do you get help from?

*

○ Internet ○ Friend ○ Colleague ○ BCS technician

7.

If the technician is helping you, do they: (please tick all the applicable)

*

☐ Come to your office

☐ Use the phone

☐ Control your computer from their office?

☐ All the above

8. While trying to resolve the problem, if you are asked for your password do you give it? *

○ Yes ○ No

9. Computer Knowledge and Acceptace

This section deals with your computer knowledge and technology acceptance.

1. Do you like using computers for work? *

Yes No

2. Are you comfortable with computer technologies? *

Yes No

3. How do you feel about the technician taking control of your computer from their office? *

very comfortable Comfortable Neutral Unease Very unease

4. Do you think you are the only one with access to your information on work computers? *

Yes No Maybe

5. Can technicians be trusted? *

Yes No Maybe

6. Do you appreciate a new version when it is released? *

Yes No

7. To what extent do you trust your web browser to auto-complele the URL (Internet address) for you? *

Always

Often

Sometimes

Rarely

Not at all

8. To what extent do you use your computer for the following: *

	Always	Sometimes	Not at all
Communication			
Research			
Teaching			
Administration			
Internet browsing			
Internet banking			
Downloading notes, games, programs, movies and music			
playing games, music, Skype			
Other			

APPENDIX A2: PERMISSION TO CONDUCT STUDY

End-User Security Survey Agreement

This document is an agreement between the Polytechnic of Namibia Bureau of Computer Services hereafter referred to as PON and Fungai Bhunu Shava with regard to the End user Security Survey, the PON hereby acknowledges and agrees:

1. That Fungai Bhunu Shava will perform an End User Security Survey that will identify user behavior towards application security in the PON network from the 24th May 2012 to 29 June 2012

2. That the PON has the legal right to check the contents of the survey tool for any ethical violations.

3. That Fungai Bhunu Shava will not divulge any information about the PON security she received as a result of this end user security survey. All results are confidential and will be treated as such.

4. The survey findings will be provided to the PON Bureau of Computer Services as a written report.

The PON agrees that Fungai Bhunu Shava will conduct the end user security survey among the polytechnic community and that the survey will include gathering information about end users': knowledge of security threats you are exposed to when they connect to the network; awareness of computer security policies at PON; with security interaction; Security technology/ solutions usage; primary programs for their tasks at work; knowledge of security features embedded in your Application Programs and Operating System and how they behave towards security alerts.

Signed for and on behalf of PON,

Name L. Evrard

Date 24/05/2012

Signature P.P.

Fungai Bhunu Shava

Date 24/05/2012

Signature

APPENDIX A3: COVER LETTER

Polytechnic of Namibia

Private Bag 13388, Windhoek

13 Storch Street,

Windhoek West

Date,

Dear colleague,

Objective: To carry out a pilot study survey to assess the computer security status at P.o.N.

A lecturer (busy with her Doctorate studies) in the Computer Systems and Networks Department in collaboration with the Bureau of Computer Services (BCS) is studying Computer information security culture in the organisation, focusing on ways to improve your experience with Application program Security.

In order to understand how the Polytechnic of Namibia community handles security issues related your computer information and to reduce the risk of losing it, we are busy with a pilot study. The survey will gather information about:

1. Your knowledge of security threats you are exposed to when you connect to the network.
2. Your awareness of computer security policies in the organisation.
3. Your experiences with security interaction.
4. Security technology/ solutions usage among the community members.
5. The programs you are using for primary tasks at work/ job.
6. Your knowledge of security features embedded in your Application Programs and Operating System.
7. How you behave towards security alerts.

Please answer the questions as honestly as possible; the information gathered from this will be used to improve the information security in our organisation. It is not intended to assess your computer knowledge. The results of this survey will be used to enhance your information security by considering your experience with application programs. Please feel free to include any information you think will be of help to us. The results will be confidential. Your input will

be greatly appreciated as it will influence how we address your concerns. Your usual cooperation is highly appreciated.

Thank you for your cooperation.

Yours sincerely

Fungai Bhunu Shava

APPENDIX A4: SEMI-STRUCTURED INTERVIEWS

Structured interviews

End user

1. To what extent do you feel that the security alerts/ dialogues displayed to you are:
    a. Annoying
    b. Time wasting
    c. Too long
    d. Vague
    e. Helpful
2. Do you like interacting with them?
3. Of the programs you use, which one displays its security dialogues in a favourable way?
4. How does the above mentioned program present the dialogues?
5. How do you think it can be improved?
6. Do you get the relevant technical support from the BCS?

IT/Technical staff

1. To what extent do you think the user is responsible for security problems usually experienced in the network? (viruses, social engineering, hacking…)
   Always, sometimes, never.
2. Why is this a problem?
3. In your own opinion, how can it be fixed?
4. Do you think users at poly are not behaving responsibly?
5. What policies are directly related to the users?
6. Do organisational policies allow users to be in control of their own security? (can they update software? Can they install plugins?)

APPENDIX A5: SURVEY RESULTS SUMMARY

End User Information Security Survey

Page 1. Introduction

1. Which school/Department are you in?

Number of Respondents	58
Number of respondents who skipped this question	0

2. What is your gender?

	% of Respondents	Number of Respondents
Female	43.10%	25
Male	56.90%	33
Number of respondents		*58*
Number of respondents who skipped this question		*0*

3. How long have you been in the Organisation?

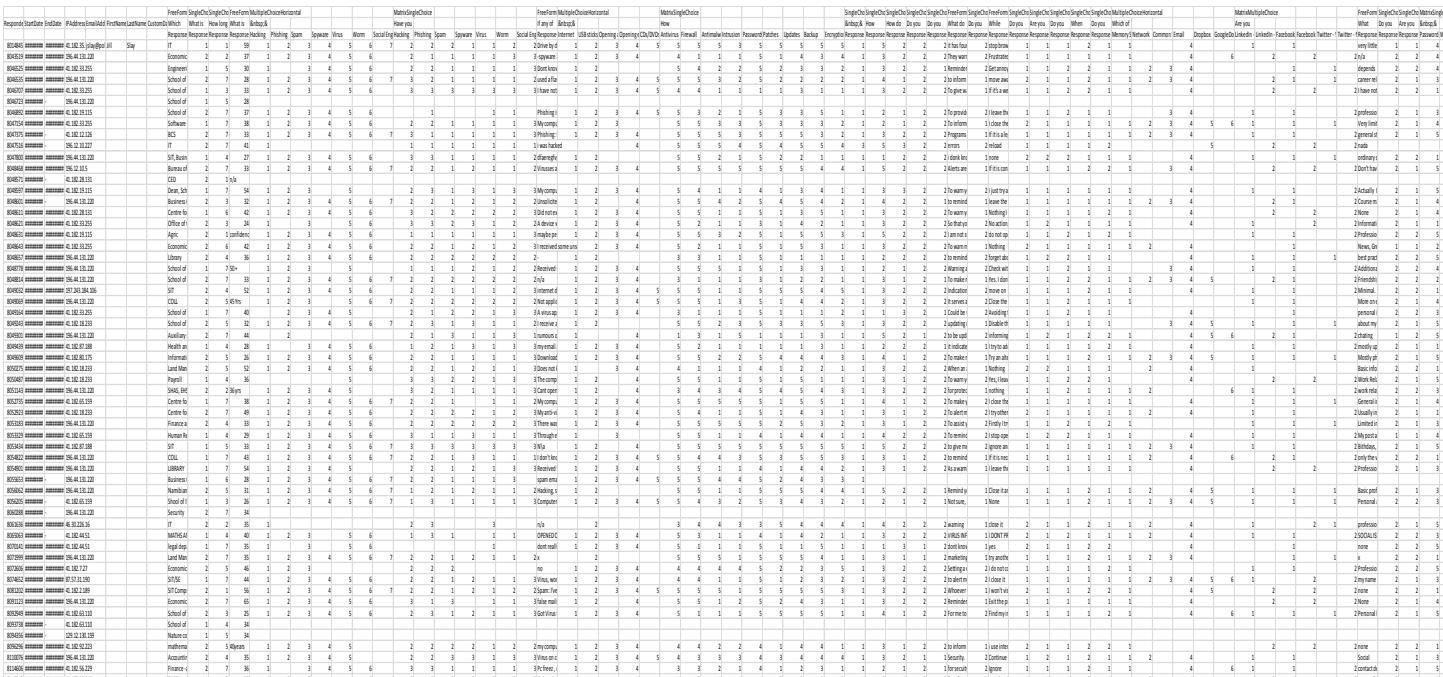
	% of Respondents	Number of Respondents
0- 6 Months	6.90%	4
6-12 Months	5.17%	3
1 Year +	10.34%	6
2 Years +	17.24%	10
3 Years +	18.97%	11
4 Years +	5.17%	3
5 Years +	36.21%	21
Number of respondents		*58*
Number of respondents who skipped this question		*0*

4. What is your age?

Number of Respondents	58
Number of respondents who skipped this question	0

Page 2. User Information Security Awareness

APPENDIX A6: SURVEY RAW DATA



APPENDIX B1: CHECKLIST FOR ADOBE READER

Security and user experience evaluation

The purpose of the evaluation is to determine the awareness of and UX of the embedded security features in Adobe.

Please select or fill in the most appropriate response.

Post graduate study:		Research Area:					
M	D	USec	InfoSec	UX	HCI	Application Development,	Application Evaluation

Tasks

Please perform the following seven tasks in Adobe and select the most appropriate category on the checklist presented in table 2.

1. Password protect your document
2. Restrict editing , grant edit permissions to 1 person
3. Mark the document as final
4. Sign the file
5. Initialise every page
6. Time stamp the file
7. Encrypt your file
8. Share the file as read only
9. Remove the protection

Procedure

Perform the nine tasks above and evaluate your security and experience. The following options may be used to evaluate the end user program user experience and security:

- **Yes**: If one agrees with the checklist item in relation to the application.
- **No**: If one disagrees with the checklist item in relation to the application.
- **NA** (Not Applicable): If one believes that the checklist item is not applicable to the website/application.

Note

- **Ext** (extent): used to measure the extent of aspect as a value between 1(very difficult) and 5 (very easy).
- **Comments**: available for one to enter additional comments relating to the specific checklist item and how it relates to the end user program

1. Visibility/Findable/locatable/ readily displayed – the security feature must be easily found					
Checklist Items	Yes	No	N/A	Ext	Comments
1.1. Can you easily locate the security feature					
1.2. After completing a security action, do you get some form of feedback					
1.3. Can you disable the security feature?					
2. Motivating – the security feature must encourage users to re- use it again in future					
Checklist Items	Yes	No	N/A	Ext	Comments
2.1. Are you motivated to use it again					
2.2. Will you recommend it to others					
2.3. Does it satisfy your perceived goals					
3. Desirable– the security feature must be pleasant to use, and look at					
Checklist Items	Yes	No	N/A	Ext	Comments
3.1. Is the presentation visually appealing?					
3.2. Is the feature pleasant to use?					
4. Useful- the security features must enable the user to achieve security goals willingly.					
Checklist Items	Yes	No	N/A	Ext	Comments
4.1. Helps me to be secure					
4.2. They protect my work					
4.3. It does everything I would expect it to do.					
5. Learnability/ understandable, ease of use – the system should ensure that security actions are easy to learn and remember					
Checklist Items	Yes	No	N/A	Ext	Comments
5.1. The security features have been grouped into logical zones, and have headings been used to distinguish them from other program features					
5.2. I learned how to use the security feature easily					
5.3. The security features are easy to remember					
5.4. Menus make obvious which security items are selected					
5.5. The program protect you from making errors					
5.6. Security-related information is presented in a standardized manner					
6. Aesthetics and Minimalist Design – the system should offer users relevant information relating to their security actions					
Checklist Items	Yes	No	N/A	Ext	Comments

6.1. Only the security information essential to decision making is displayed on the screen?					
6.2. All security icons in a set are visually and conceptually distinct					
6.3. Security labels are brief, familiar and descriptive?					
7. Exciting/emotion/perception – the program should excitement and good perceptions/ emotions					
Checklist Items	Yes	No	N/A	Ext	Comments
7.1. You feel excited about the security features					
7.2. You perceive them as good					
7.3. Security task evoke positive emotions in you					
7.4. The security-related error messages are accurate in their descriptions?					
7.5. It was enjoyable to perform security functions					
8. Satisfaction – the system should ensure that users have a good experience when using security and that they are in control					
Checklist Items	Yes	No	N/A	Ext	Comments
8.1. Security features are easy to work with					
8.2. You feel disturbed when you perform security tasks					
8.3. Security-related prompts imply that you are in control?					
8.4. You are satisfied with the security					
9. User Suitability – the system should provide options for users with diverse levels of skill and experience in security					
Checklist Items	Yes	No	N/A	Ext	Comments
9.1. Do the security features support both novice and expert users; are multiple levels of security error messages detail available?					
9.2. Can you easily change the level of security detail?					
9.3. Can you easily change between novice and expert levels?					
9.4. Can you customize security to meet your individual preferences?					
10. Comfortable to use /User Language – the system should use plain language that users can understand with regards to security					
Checklist Items	Yes	No	N/A	Ext	Comments
10.1. Are security actions named consistently across all prompts in the program?					

10.2. Is security information accurate, complete and understandable?					
10.3. Are security messages stated in clear and simple language, where used?					
10.4. Is security jargon avoided?					
11. User Assistance/ Help – the system should make security help apparent for users					
Checklist Items	Yes	No	N/A	Ext	Comments
11.1. Is there a security help function visible (e.g. a key labelled "Security Help")?					
11.2. Is the security information provided relevant?					
11.3. Can users easily switch between security help and their work?					
11.4. Do instructions follow the sequence of user security actions?					
11.5. Does the system provide users with updated security educational opportunities, if they desire it?					
12. Efficiency the security feature must complete the user's goal in a timely and accurate manner					
12.1. Was it easy to enforce security?					
12.2. It takes long to compete the tasks					
12.3.					
13. Accessible – the security feature must be reachable to accomplish a security objective					
Checklist Items	Yes	No	N/A	Ext	Comments
13.1. Does not present technical or physical barriers					
13.2. Readily accessible					
14. Effective - the extent to which the security feature fulfils the users' expectations with ease .					
Checklist Items	Yes	No	N/A	Ext	Comments
14.1. Does what it supposed to do					
14.2. Fulfils my security needs					
15. Usable- the security features must allow the user to do what they want to do in the way they expect to do it without difficulty, hesitancy, or queries					
Checklist Items	Yes	No	N/A	Ext	Comments
15.1. Is it convenient to use					
15.2. It is simple to use					
15.3. Is it doing the expected					
16. Valuable/ impact of use – the security feature should relate to the user goals in a beneficial					

way					
Checklist Items	Yes	No	N/A	Ext	Comments
16.1. It secures my documents					
16.2. You are not losing information					
16.3. Your files are not edited by wrong people?					
16.4. It does not waste my time?					
16.5. Assures you of the file author?					
17. Security – the system needs to consider integrity, availability, confidentiality, auditing and non-repudiation					
Checklist Items	Yes	No	N/A	Ext	Comments
17.1. The information is only accessible to authorised users					
17.2. Protected or confidential information can be accessed only with valid authentication					
17.3. The program encrypts the whole file					
17.4. You can update or delete document properties information					
17.5. The program notifies you of your access privileges?					
17.6. The program protects all files downloaded					
17.7. Does the program disable macros?					
17.8. Are notification messages relating to security displayed to the user before access to the system is granted?					
17.9. Are the controls for sharing readily available?					
17.10. Does the program install required software updates automatically and notify you about this action?					
17.11. Does the program display options to assist in the reporting of security incidents?					
17.12. Does the program notify you of any vulnerability associated with not applying security?					
17.13. Does the program notify you about auto recovery?					
18. Awareness/Expected security features must be expected the programs, users should be aware of their existence					
18.1. Does the system provide awareness and educate you on how to complete tasks?					

18.2.	Do you expect the security features?					
18.3.	Are you aware of the location of the security features in the program?					
18.4.	Are you aware of the limitations of the security?					
18.5.	Are you aware of the effect of applying security?					
18.6.	Are you educated on proper security usage?					

APPENDIX B2: CHECKLIST FOR MS WORD

Security and user experience evaluation

The purpose of the evaluation is to determine the awareness of and UX of the embedded security features in MS Word.

Please select or fill in the most appropriate response.

Post graduate study:		Research Area:					
M	D	USec	InfoSec	UX	HCI	Application Development,	Application Evaluation
	x	x		x	x		

Tasks

Please perform the following seven tasks in MS Word and select the most appropriate category on the checklist presented in the table below.

10. Password protect your document
11. Restrict editing , grant edit permissions to 1 person
12. Mark the document as final
13. Sign the file
14. Encrypt your file – similar to password protect document
15. Share the file as read only
16. Remove the protection – could not remove password

Procedure

Perform the seven tasks above and evaluate your security and experience. The following options may be used to evaluate the end user program user experience and security:

- **Yes**: If one agrees with the checklist item in relation to the application.
- **No**: If one disagrees with the checklist item in relation to the application.
- **NA** (Not Applicable): If one believes that the checklist item is not applicable to the website/application.

Note

- **Ext** (extent): used to measure the extent of aspect as a value between 1(very difficult) and 5 (very easy).
- **Comments**: available for one to enter additional comments relating to the specific checklist item and how it relates to the end user program

19. Visibility/Findable/locatable/ readily displayed – the security feature must be easily found					
Checklist Items	Yes	No	N/A	Ext	Comments
19.1. Can you easily locate the security feature					
19.2. After completing a security action, do you get some form of feedback					
19.3. Can you disable the security?					
20. Motivating – the security feature must encourage users to re- use it again in future					
Checklist Items	Yes	No	N/A	Ext	Comments
20.1. Are you motivated to use it again					
20.2. Will you recommend it to others					
20.3. Does it satisfy your perceived goals					
21. Desirable– the security feature must be pleasant to use, and look at					
Checklist Items	Yes	No	N/A	Ext	Comments
21.1. Is the presentation visually appealing?					
21.2. Is the feature pleasant to use?					
22. Useful- the security features must enable the user to achieve security goals willingly.					
Checklist Items	Yes	No	N/A	Ext	Comments
22.1. Helps me to be secure					
22.2. They protect my work					
22.3. It does everything I would expect it to do.					
23. Learnability/ understandable, ease of use – the system should ensure that security actions are easy to learn and remember					
Checklist Items	Yes	No	N/A	Ext	Comments
23.1. The security features have been grouped into logical zones, and have headings been used to distinguish them from other program features					
23.2. I learned how to use the security feature easily					
23.3. The security features are easy to remember					
23.4. Menus make obvious which security items are selected					
23.5. The program protect you from making errors					
23.6. Security-related information is presented in a standardized manner					

24. Aesthetics and Minimalist Design – the system should offer users relevant information relating to their security actions					
Checklist Items	Yes	No	N/A	Ext	Comments
24.1. Only the security information essential to decision making is displayed on the screen?					
24.2. All security icons in a set are visually and conceptually distinct					
24.3. Security labels are brief, familiar and descriptive?					
25. Exciting/emotion/perception – the program should excitement and good perceptions/ emotions					
Checklist Items	Yes	No	N/A	Ext	Comments
25.1. You feel excited about the security features					
25.2. You perceive them as good					
25.3. Security task evoke positive emotions in you					
25.4. The security-related error messages are accurate in their descriptions?					
25.5. It was enjoyable to perform security functions					
26. Satisfaction – the system should ensure that users have a good experience when using security and that they are in control					
Checklist Items	Yes	No	N/A	Ext	Comments
26.1. Security features are easy to work with					
26.2. You feel disturbed when you perform security tasks					
26.3. Security-related prompts imply that you are in control?					
26.4. You are satisfied with the security					
27. User Suitability – the system should provide options for users with diverse levels of skill and experience in security					
Checklist Items	Yes	No	N/A	Ext	Comments
27.1. Do the security features support both novice and expert users; are multiple levels of security error messages detail available?					
27.2. Can you easily change the level of security detail?					
27.3. Can you easily change between novice and expert levels?					
27.4. Can you customize security to meet your individual preferences?					

28. Comfortable to use /User Language – the system should use plain language that users can understand with regards to security					
Checklist Items	Yes	No	N/A	Ext	Comments
28.1. Are security actions named consistently across all prompts in the program?					
28.2. Is security information accurate, complete and understandable?					
28.3. Are security messages stated in clear and simple language, where used?					
28.4. Is security jargon avoided?					
29. User Assistance/ Help – the system should make security help apparent for users					
Checklist Items	Yes	No	N/A	Ext	Comments
29.1. Is there a security help function visible (e.g. a key labelled “Security Help”)?					
29.2. Is the security information provided relevant?					
29.3. Can users easily switch between security help and their work?					
29.4. Do instructions follow the sequence of user security actions?					
29.5. Does the system provide users with updated security educational opportunities, if they desire it?					
30. Efficiency the security feature must complete the user’s goal in a timely and accurate manner					
30.1. Was it easy to enforce security?					
30.2. It takes long to compete the tasks					
30.3.					
31. Accessible – the security feature must be reachable to accomplish a security objective					
Checklist Items	Yes	No	N/A	Ext	Comments
31.1. Does not present technical or physical barriers					
31.2. Readily accessible					
32. Effective - the extent to which the security feature fulfils the users’ expectations with ease .					
Checklist Items	Yes	No	N/A	Ext	Comments
32.1. Does what it supposed to do					
32.2. Fulfils my security needs					
33. Usable- the security features must allow the user to do what they want to do in the way they expect to do it without difficulty, hesitancy, or queries					
Checklist Items	Yes	No	N/A	Ext	Comments

33.1. Is it convenient to use					
33.2. It is simple to use					
33.3. Is it doing the expected					
34. Valuable/ impact of use – the security feature should relate to the user goals in a beneficial way					
Checklist Items	Yes	No	N/A	Ext	Comments
34.1. It secures my documents					
34.2. You are not losing information					
34.3. Your files are not edited by wrong people?					
34.4. It does not waste my time?					
34.5. Assures you of the file author?					
35. Security – the system needs to consider integrity, availability, confidentiality, auditing and non-repudiation					
Checklist Items	Yes	No	N/A	Ext	Comments
35.1. The information is only accessible to authorised users					
35.2. Protected or confidential information can be accessed only with valid authentication					
35.3. The program encrypts the whole file					
35.4. You can update or delete document properties information					
35.5. The program notifies you of your access privileges?					
35.6. The program protects all files downloaded					
35.7. Does the program disable macros?					
35.8. Are notification messages relating to security displayed to the user before access to the system is granted?					
35.9. Are the controls for sharing readily available?					
35.10. Does the program install required software updates automatically and notify you about this action?					
35.11. Does the program display options to assist in the reporting of security incidents?					
35.12. Does the program notify you of any vulnerability associated with not applying					

	security?					
35.13.	Does the program notify you about auto recovery?		x			
36.	Awareness/Expected security features must be expected the programs, users should be aware of their existence					
36.1.	Does the system provide awareness and educate you on how to complete tasks?					
36.2.	Do you expect the security features?					
36.3.	Are you aware of the location of the security features in the program?					
36.4.	Are you aware of the limitations of the security?					
36.5.	Are you aware of the effect of applying security?					
36.6.	Are you educated on proper security usage?					

APPENDIX B3: CROSS COMPARISON OF ADOBE AND MS WORD

Visibility/Findable/locatable/readily displayed; the security feature must be easily found		
	Adobe	**Word**
Can you easily locate the security feature	9/14	12/15
After completing a security action, do you get some form of feedback	10/14	12/15
Can you disable the security?	10/14	9/14
Motivating- the security feature must encourage users to re- use it again in future		
Are you motivated to use it again	9/14	10/15
Will you recommend it to others	10/14	12/15
Does it satisfy your perceived goals	8/14	11/15
Desirable- the security feature must be pleasant to use, and look at		
Is the presentation visually appealing?	8/13	9/15
Is the feature pleasant to use?	7/13	9/15
Useful- the security features must enable the user to achieve security goals willingly.		
Helps me to be secure	11/14	12/15
They protect my work	11/14	14/15
It does everything I would expect it to do	5/14	7/15
Learnability/understandable, ease of use -the system should ensure that security actions are easy to learn and remember		
The security features have been grouped into logical zones, and have headings been used to distinguish them from other program features	9/14	13/15
I learned how to use the security feature easily	10/14	11/15
The security features are easy to remember	8/14	12/15
Menus make obvious which security items are selected	7/14	10/15
The program protect you from making errors	7/14	5/15
5.6. Security-related information is presented in a standardized manner	9/14	8/15
Aesthetics and Minimalist Design; the system should offer users relevant information relating to their security actions		
Only the security information essential to decision making is	5/14	10/14

displayed on the screen?		
All security icons in a set are visually and conceptually distinct	9/14	8/15
Security labels are brief, familiar and descriptive?	9/14	12/15
Exciting/emotion/perception- the program should excitement and good perceptions/ emotions		
You feel excited about the security features	8/14	6/15
You perceive them as good	11/14	12/15
Security task evoke positive emotions in you	10/14	8/15
The security-related error messages are accurate in their descriptions?	11/14	11/15
It was enjoyable to perform security functions	8/14	9/15
Satisfaction- the system should ensure that users have a good experience when using security and that they are in control		
Security features are easy to work with	8/14	9/15
You feel disturbed when you perform security tasks	2/14	3/15
Security-related prompts imply that you are in control?	11/14	9/15
You are satisfied with the security	8/14	11/14
User Suitability - the system should provide options for users with diverse levels of skill and experience in security		
Do the security features support both novice and expert users; are multiple levels of security error messages detail available?	5/14	7/15
Can you easily change the level of security detail?	7/14	7/15
Can you easily change between novice and expert levels?	3/14	3/15
Can you customize security to meet your individual preferences?	8/14	11/15
Comfortable to use /User Language -the system should use plain language that users can understand with regards to security		
Are security actions named consistently across all prompts in the program?	8/13	10/15
Is security information accurate, complete and understandable?	8/13	10/15
Are security messages stated in clear and simple language, where used?	8/13	10/15

Is security jargon avoided?	6/13	9/14
User Assistance/ Help - the system should make security help apparent for users		
Is there a security help function visible (e.g. a key labelled "Security Help")?	6/14	4/15
Is the security information provided relevant?	10/14	11/15
Can users easily switch between security help and their work?	8/14	8/15
Do instructions follow the sequence of user security actions?	10/14	9/15
Does the system provide users with updated security educational opportunities, if they desire it?	3/14	3/15
Efficiency the security feature must complete the user's goal in a timely and accurate manner		
Was it easy to enforce security?	5/14	9/14
It takes long to compete the tasks	5/14	6/14
Accessible- the security feature must be reachable to accomplish a security objective		
Does not present technical or physical barriers	11/14	12/14
Readily accessible	10/14	10/14
Effective- the extent to which the security feature fulfils the users' expectations with ease.		
Does what it supposed to do	9/14	13/14
Fulfils my security needs	814	11/14
Usable- the security features must allow the user to do what they want to do in the way they expect to do it without difficulty, hesitancy, or queries		
Is it convenient to use	9/14	12/15
It is simple to use	8/14	13/15
Is it doing the expected	10/14	13/15
It secures my documents	10/14	14/14
You are not losing information	8/14	12/14
Your files are not edited by wrong people?	9/14	12/14
It does not waste my time?	11/14	8/14
Assures you of the file author?	8/14	7/11
Security- the system needs to consider integrity, availability, confidentiality, auditing and		

non-repudiation		
The information is only accessible to authorised users	12/14	12/14
Protected or confidential can information be accessed only with valid authentication	12/14	13/15
The program encrypts the whole file	11/14	9/15
You can update or delete document properties information	9/14	13/15
The program notifies you of your access privileges?	8/14	11/15
The program protects all files downloaded	6/14	7/15
Does the program disable macros?	2/14	5/15
Are notification messages relating to security displayed to the user before access to the system is granted?	7/14	10/15
Are the controls for sharing readily available?	6/14	9/15
Does the program install required software updates automatically and notify you about this action?	7/14	6/15
Does the program display options to assist in the reporting of security incidents?	5/14	6/15
Does the program notify you of any vulnerability associated with not applying security?	4/14	4/15
Does the program notify you about auto recovery?	5/14	8/14
Awareness/Expected security features must be expected the programs, users should be aware of their existence		
Does the system provide awareness and educate you on how to complete tasks?	3/14	3/15
Do you expect the security features?	9/14	12/14
Are you aware of the location of the security features in the program?	12/14	13/15
Are you aware of the limitations of the security?	8/14	8/15
Are you aware of the effect of applying security?	14/14	15/15
Are you educated on proper security usage?	10/14	11/15

APPENDIX C1: CONFERENCE PAPER 1

Factors affecting user experience with security features: A case study of an academic institution in Namibia

Fungai Bhunu Shava

PhD I.T. student Nelson Mandela Metropolitan University
Lecturer Polytechnic of Namibia
Windhoek, Namibia
fbshava@polytechnic.edu.na

Professor Darelle Van Greunen
Faculty of Engineering, Built Enviroment and ICT, School of ICT, Institute for ICT Advancement, Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Darelle.vanGreunen@nmmu.ac.za

Abstract

The widespread use of personal computers and other devices based on Information and Communication Technology (ICT) for networking and communication via the Internet exposes the end users to cybercriminals. Security systems and security features that interact with users via alerts, dialogue boxes and action buttons (such as update notices and other warnings) are embedded in operating systems and application programs in order to protect electronic information. Human behaviour and attitudes towards security features determine the user experience during the implementation of Information Security. Cyber criminals are primarily targeting the human aspect of security, since end users are easier to manipulate. In order to effectively secure information, the fields of Usable security and User experience should be integrated in the design and use of security features. This paper presents the findings of an online survey carried out to investigate attitudes towards, behaviour with and experience of embedded security features among members of staff in a tertiary education institution. User experience was measured by enumerating general security awareness, policy awareness and implementation, as well as user behaviour and emotions associated with security interaction. This paper reports on the findings of this survey. The researchers envisage that the findings can lead to the practical development and implementation of a framework for secure user experience.

Keywords- user experience; user behaviour; security feature; end user application program.

I. INTRODUCTION

Technology is shaping global behaviour by dictating how players must behave in order to survive the information technology age. Almost every job and communication now depends on information technology and is carried out with the aid of some application programs. Advancements in both system design and communication technologies have presented an opportunity for all to be interconnected. More end users are now connected to the Internet, including cybercriminals. This is enabled by the use of a variety of devices, some of which are mobile devices. Computers are now an integral component in homes and businesses, including in academic institutions like the one that was studied. Due to readily available network access, Africa has realised high Internet connectivity, and has an increasing number of novice end users connected to the World Wide Web. Namibia is rated as having an Internet user growth rate of 6.9% from 2000 as reported in the 2010- 2011 period [1]. With the launching of the West Africa Cable System (WACS), it is anticipated that Internet connection rates will drop allowing more Namibians to connect. This poses a security concern for the nation as cyber criminals will also find it easier to connect and also they will be presented with easier targets. To protect the end user's information, End user application programs have built in security features which interact with users to protect their information. Information security protects individual and organisation security from cyber criminals.

This paper presents the findings of an online survey carried out to investigate attitudes towards, behaviour with and experience of embedded security features among members of staff in a tertiary education institution. User experience was measured by enumerating general security awareness, policy awareness and implementation, as well as user behaviour and emotions associated with security interaction. The structure of the paper will be: User experience, Usable security, Case study, results and discussion, recommendations and conclusion.

II. USER EXPERIENCE

A. Definition

User experience (UX) is an individual's perceptions and responses as a result of use or anticipated use of a product, system or service [2]. For our studies we will adopt the alternative definition by [3] which defines UX as:

"a consequence of a user's internal state (e.g. predispositions, expectations, needs, motivation, mood, etc.), the characteristics of the designed system (e.g. complexity, purpose, usability, functionality, etc.) and the context (or the environment) within which the interaction occurs (e.g. organisational/social setting, meaningfulness of the activity, voluntariness of use, etc.)".

978-1-4799-0808-0/13/$31.00 ©2013 IEEE

It is a discipline that falls in the field of Human-computer Interaction (HCI). User experience design (UXD) focuses on the emotional aspects of human experience such as happiness, although it is closely related to User-Centered Design (UCD) methods, which target human performance enhancement [4]. Since user experience refers to the overall perceptions of end users (effectiveness, efficiency, emotional satisfaction, quality of relationship with service entity) as they interact with a product or service [5], it is important that the design focuses on embracing all these factors in the security features.

A. End user experience

End users' perception of application program quality is based on their experience of interaction, as well as on those application program qualities that give rise to effective use and pleasure [6]. In order to have the complete picture of end user experience, it is necessary to consider the user's characteristics (such as skills, background, personality, motives and cultural values), product qualities (usability, appeal, behaviour) and the environment in which the interaction takes place [7], [3].

B. Usage Factors

Herzog and Shahmehri [8] realised that program security has features that influence the behaviour of users towards the execution or implementation of such features. It is important that designers focus on how to affect the user in a positive way. Studies conducted by [9], [10] show that it is possible to realign security and usability with careful attention to UCD principles, and make security usable. The question is: what characteristics does an application program have and how do they affect the user? Also: what characteristics does a user have that influence their experience with security features? We can look at how the environment, security culture and duties of the application program user shape their emotions when confronted with a dialogue that requires them to act in a secure manner.

Hassenzahl [3] came up with a model of UX which describes the designer's as well as the user's perspectives of product features. A designer has an intended product character on development, and puts up guidelines for the user to follow in order to get the desired experience. However because the user has characteristics that shapes how they perceive the product, the actual product character they encounter is different from the intended, in turn this evokes different consequences. We need to evaluate the extent of positive or negative feelings that can be experienced by end users in a particular environment, during and after interaction with the product. We also need to explore and how that influences further usage [6]. The evaluation helps us to determine how the interaction with security features can be guided to ensure a "degree to which specified users can achieve actual usability, safety, and satisfaction in use in a specified context of use" [11].

In order to evaluate the effect of a program's security feature on UX, various criteria that influence the overall UX can be used. Some important aspects are security policies, usability (convenience, efficiency, understandable, visibility) [12] user knowledge of security threats and solution and/or mitigation strategies related to their application programs. Giovanni [13] states that end user behaviour is directly linked to emotional satisfaction. It is against these factors that the researchers designed a survey to capture information on users' awareness of ICT security policies, their knowledge of security threats and solutions, the feelings invoked by interaction with security features and the behaviour that results from the feeling.

III. Usable Security

Usable Security (USec) also known as HCI security is the field that deals with human issues and Information Security, focusing on the design of security that is usable. It is defined as "A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users" [2].

A. Characteristics

The characteristics of USec include learnability, understandability, operability, efficiency, effectiveness and user satisfaction [14], [5]. Furnell [10] Investigated desirable characteristics of security such as locatable, understandable, convenient and visible; and realised that too usable can mean easy to compromise. A need to establish a balance between usability and complexity therefore exits. Furnell [10] also noted that there is need for more to be done to understand users' needs and address them.

As far back as 2005, [9] identified that realigning security and usability with careful attention to user centered design principles, security and usability can be synergetic. This area falls under the fields of InfoSec and HCI. It is important that we examine human behaviour towards security in our quest to address problems associated with end user security. The field of HCI is concerned with the design, evaluation and implementation of interactive computing systems for human use. Literature has shown that the human element is now the key to breaking or securing the information system. To secure the information, the security features presented to the end users must be usable in a way that appeals to them.

Whitman and Mattord [15] define poor usability as the tendency of end users to always prefer the easier option, when confronted with a choice between the official way of doing a job and the easier unofficial way. For example, whenever a new program update is available, the computer will prompt the user to update through an alert but will include an option to ignore or cancel. Choosing 'yes' implies that there will be more choices to make in future, while choosing to ignore the prompt to update will require the user to only click once without any further prompting.

The work done so far has not addressed the issues influencing the security of end user experience while interacting with these features. Previous work has focused on ensuring that security features are designed to be usable. The number of breaches associated with poor usage or no usage of security features is on the rise. Efforts to provide technically robust security solutions are fruitless if the beneficiary is not able to use them. We have investigated the factors that

influence user experience with program security features, and propose the model at Figure 1 that can be used to address the missing link between usable program security and user experiences. Much has been done to realign security design with usability. However, a lot still needs to be done to enhance or cultivate a positive experience with usable security.

Yeratziotis *et al* [16] used usability criteria to evaluate two online health systems. The criterion included trust, ease of use, terminology, ease of learning, feedback, awareness, errors, help and documentation. Yeratziotis *et al* [16] concluded that designers require tools that assist them to improve USec, in light of the fact that users need usable features to assist them in effectively securing their information.

This article presents the factors that influence end users to behave in the manner which they do. Assuming that the application program designers are focusing on embedding usable security features, what is left is to ensure that the end users secure their own information as well as that of the organisation.

B. End user application programs

These are the application programs that end users employ to perform daily tasks on their computers. The most popular used application programs as documented by [12] are web browsers (Internet Explorer), email client (Outlook Express) and word processors (Microsoft Word). In another Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office were also identified as popular application programs [17].

C. Security and security features

End user application programs have embedded security features such as the update service, password options, permissions, encryption, sharing security and other program-specific features. In a survey by [12], it was found that 73% of respondents used passwords even though the operating system under study (Windows XP) has logon as a security feature. Furthermore users are supposed to use passwords for online activities and to protect their information.

End users make use of application programs to access desired services on their devices and on the Web. Application programs have thus become the most used software in the information technology (IT) age, presenting cybercriminals with yet another means of accessing and manipulating user information [15], [17]. Software developers have embedded security features and components in end user application programs, in order to interact with end user to protect their information [12]. However, many end users regard security as an administrative function that should be handled by IT experts. As such they usually ignore security-related responsibilities, due to the complex nature of security and the fact that it is not perceived to be the user's duty [8].

IV. CASE STUDY

A case study approach was followed based on the approaches defined by [18], [19], [20]. According to these authors case study research is a detailed inquiry of an issue used to evaluate the authenticity of the problem and allows researchers to gather realistic data of the phenomenon being investigated in social and behavioural scientific research.

A. Academic Institution

For the purpose of this research, a case study of the Polytechnic of Namibia (academic institution in Namibia) was conducted. The Institution is located in the nation's capital city Windhoek. It has a student enrolment of 13400 per annum and employs 670 full time staff. Every staff member has a desktop or personal computer (PC) and/or laptop allocated to them for their daily work. The student laboratories and library are equipped with PCs which are used for practical sessions as well as for information search on the internet and on e-library resources. Each PC has a Windows or Ubuntu operating system installed for the daily business activities. Laboratories mainly use Windows, although in some departments Centos, Ubuntu, or MAC OS are used. Typical application software includes Microsoft Office, Internet browsers, integrated tertiary system (ITS), document readers (Acrobat), anti-virus software (Kaspersky lab), and email clients (mainly Thunderbird).

B. Materials and methods

An exploratory case study design was used as it allows researchers to gather holistic characteristics of real occurrences, such as group behaviours, within a population[18]. A purposive, non-probabilistic method of sampling was

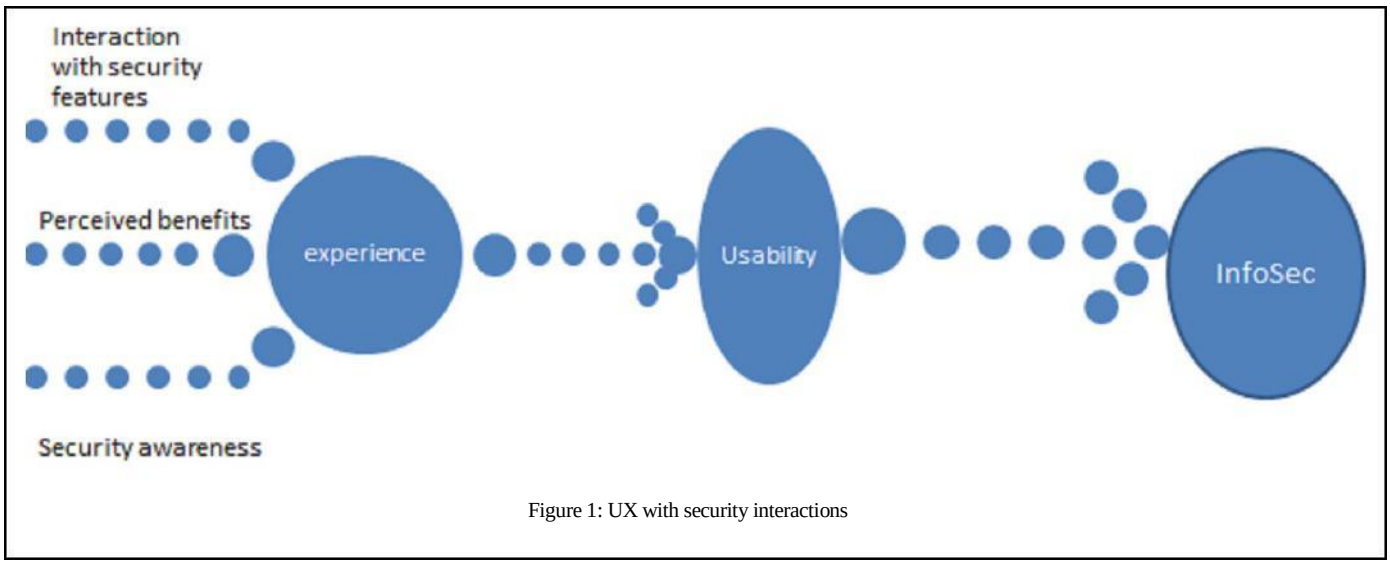


Figure 1: UX with security interactions

used, targeting the sample population staff members and aiming for a minimum of 30 responses. Qualitative data analysis was used. It requires rigorous analysis of the data, and a sample of 30 is therefore sufficient [21].

The study area was unambiguously described in the context of the case, as well as in terms of the objectives and actions to be taken [22]. The context in this case is shaped by the organisational security culture and support mechanisms that are in place. The researchers therefore looked at policing of and adherence to policies, as well as at security awareness.

The data that were gathered were classified according to exhibited patterns or characteristics, to allow for effective analysis. The classification was based on research aims and objectives. After classification of the data, we established connections among different categories. The categories form the concepts or variables for the formulation of the theoretical framework, and for the relationships that form the connections. Meanings were logically inferred from literature. Description, contextualisation, classification, processing and linking of gathered data were adopted.

C. *Procedure*

A survey was conducted in order to understand how the community handles security issues related to electronic information. In order to get an overall understanding of Information Security problems resulting from inadequate end user support, we gathered information about: end users' knowledge of the security threats to which they are exposed when they connect to networks; awareness of computer security policies in the organisation; experiences with security interaction; security technology/solutions usage among the community members; the application programs used for primary tasks at work/job; knowledge of security features embedded in application programs and operating systems; and behaviour towards security alerts.An example of a question which was asked is shown in Figure 2. The end users would tick an appropriate level of knowledge for a policy in place.

The objectives of the study were presented to the respondents in a cover letter. Based on this information, they made a voluntary informed choice whether or not to participate in the survey. Thus purposive and self-selecting sampling techniques were used. The responses were treated anonymously and in a confidential manner, thus ensuring that upon reporting or publishing no link could be made to the population studied.

3. To what extent do you know these policies? (1 is not at all and 5 is very well)

1	2	3	4	5
Password				
Wireless				
Internet				
General Computer usage				

Figure 2: Sample question

Semi structured interviews were carried out with 5 technical and 5 non-technical employees, in order to gain an understanding of the nature of the representatives of the population. Questions were open- ended so as to allow respondents to provide us with an insight into the situation. For further analysis, an online survey was designed to collect data from a population of about 670 end users using E-surveys Pro. The survey tool was pre-tested with seven users, after which it was deployed to all population members by means of a broadcast email containing the link. The online survey is quick and inexpensive to administer. It furthermore saves time in analysis as the data can be electronically analysed using statistical tools.

D. *Participant selection*

The participants in this research comprised of lecturers, administrators and other professionals who make up the university community. The institution has 670 full time employees. The population was chosen in order to reflect a diversity of users from different backgrounds and professions, who use similar application programs for similar purposes to achieve different objectives. Students were not included as the study was aimed at reflecting on a typical composition of employees in organisation.

Out of the 53 respondents who completed the survey, 23 were female and 30 were male hence there was no gender bias. The respondent composition was representative of the university employee population, and spreading across the different faculties and centres in the institution.

Data Analysis method

Responses from a sample of respondents (53) were analysed for patterns that demonstrate how the users think and feel about embedded security features in the application programs that they use. After this analysis, we recommended mechanisms to ensure positive experiences for users while using the security features.

To evaluate UX we followed a hierarchical approach described by [13] which presents three stages, namely:

- Using general knowledge to provide a basic sense of end user program security awareness and usage;
- Understanding user behaviour to determine what users are doing and where a problem exists; and
- Influencing users by determining if a security feature is compelling through measuring the emotion associated with the feature.

To gauge the security culture of the organisation, general security information was gathered. The information captured the understanding of security, threats and solutions as well as whether the end users were implementing them or not. We then assessed the behaviour of end users with security feature/ technology and the reasons for the specific behaviour. In order to fully comprehend the situation, the emotions of users associated with their interactions were also analysed.

V. Results and Discussion

A. Overview

The results are based on an inductive analysis of: security threats and solution awareness; user behaviour while interacting with security features; user attitudes and feelings towards security and the security policies that are in place. The interpretations are supported by extracts of actual responses.

A critical review of the literature has established that Information Security problems are largely due to a user's behaviour towards security features and perceptions of program security.

The survey findings indicate that many factors such as a lack of knowledge, awareness, prioritisation of work targets and misconception of security threats affect the experience of the end user with security. This experience in turn influences the tendency not to secure information. The following sections present results according to the sections of the questionnaire.

1. Systems Implemented

Table 1 shows that in our study population, the computer is mainly used as a tool for communication, for this task Thunderbird and Pronto Webmail are implemented. A variety of tools are used for research varying for the different disciplines and individual preferences. For Internet browsing several browsers are implemented including the default Windows browser Internet Explorer, Mozilla Firefox, Opera and Google Chrome. ELearning is implemented using Moodle and library services are electronic. Organisational Administration at all levels is implemented on the Integrated Tertiary system (ITS). The application programs used are mainly Microsoft products and open source software.

TABLE 1:Primary use of the computer

	$ Always	$ Sometime	$ Not At All
Communication	87	13	0
Research	85	15	0
Teaching	57	38	4
Administration	51	47	2
Internet Browsing	83	17	0
Internet Banking	53	30	17
Downloads	40	34	26
Music, Skype, Games	17	51	32
Other	17	47	36

TABLE 2: Percentage Program Usage

	$ Always	$Sometimes	$ Not at all
Word processor	86	10	4
SpreadSheets	62	36	2
Presentation	62	36	2
Graphics	20	56	24
Project management	4	30	66
Document readers	50	28	22
Database management	18	42	40
Email	100	0	0
Web browsers	92	6	2
ITS	68	30	2
Other	26	52	22

2. Frequently used Application Programs

The most popular application programs are email clients which are used by 100% of respondents, followed by Web browsers at 92%, and word processors at 86%. ITS is used by 68% of respondents, followed by spread sheets and presentation software both at 62%. The document readers are used by 50% of the respondents, whilst the remaining programs are seldom used, as is shown in Table 2. The findings favourably compare with those articulated by [12], [17].

A diversity of email clients are in use, which is contrary to the expectation. The organisation under study uses CommuniGate pro (Pronto webmail) and Thunderbird as email clients. Findings indicate the use of several other email clients including Windows Live mail. Nine per cent of respondents selected other email clients and specified Pronto, which implies that there are 17 respondents (35%) using CommuniGate. Sixty-five per cent of respondents do not know that they use Pronto on a daily basis.

B. Factors

This section presents the findings about the factors which were studied.

1. Knowledge of security threats

The users are generally aware of the Information Security threats to which they are exposed., The survey showed awareness as high as 94% for hacking and as low as 30% for social engineering, other threats such as phishing, spam, spyware, viruses and worms were in the range of 74% to 92%.

However, only 13% of the respondents knew that they had been hacked, 24% were not sure and the remaining 63% knew they had not been hacked. Hacking is the act of gaining access to electronic information illegally [15]. It is quite likely that they do not understand how hacking is carried out, and that they can therefore not detect it. Of the 92% who are aware of what spam is, 64% knew that they have been victims thereof. The same trend is observed for all the other threats.

Further enquiry showed that 68% of the users were aware that their email programs handle spam. With this level of awareness, it is tempting to assume that they know how to handle their emails. However, 44% would open emails from unfamiliar sources and 29% opens all attachments that they receive.

Despite the fact that passwords are one of the most used security methods, and that users (over 70%) know how to implement them, 40% of users will disclose their passwords to the "support" personnel when confronted with a problem. Support is in these cases offered telephonically or via remote desktop managers. Users do not have a perception of the implications of disclosing their passwords. This indicates that there is no user training on Information Security, as is confirmed by 92% of the participants.

2. Security Policy awareness

Policy awareness is the key to successful implementation of security systems, in this study at most 29% of the participants know of the policies that exist in the organisation. Twenty-nine percent know about the password policy, followed by 23% of respondents that are aware of the Internet policy. The general computer usage policy is known by 21% of the sample population, and only 13% have knowledge of the wireless policy. Ironically, every staff member has a computer for their work, and all academic staff also have a laptop that connects both to the wired and wireless networks in the organisation. Out of those who know about policies, 45% learnt about them from the Rights office and the rest from a colleague or friend. These results show that users are not aware of the existence and proper usage of policies, and that the application thereof is hence not executed. User behaviour further indicates that there is no adherence to policies when users are confronted with computer-related problems. The official process is to seek help from Computer Services. However, about 42% of users seek help from the most untrusted sources of information such as the Internet, friends or colleagues. The general computer usage policy states that all sensitive information should be encrypted; however, the survey shows that only 15% of the respondents use the facility.

3. User experience with security interaction

The end users acknowledge that they receive security alerts and that they appreciate receiving system feedback. Security features from the point of view of the designers are meant to be usable. However, 63% of respondents have negative feelings with respect to notifications, especially when they are required to act on them (58%). Figure 3 shows some of the feelings that they experience with these interactions (such as disruptive, irritating and annoying).

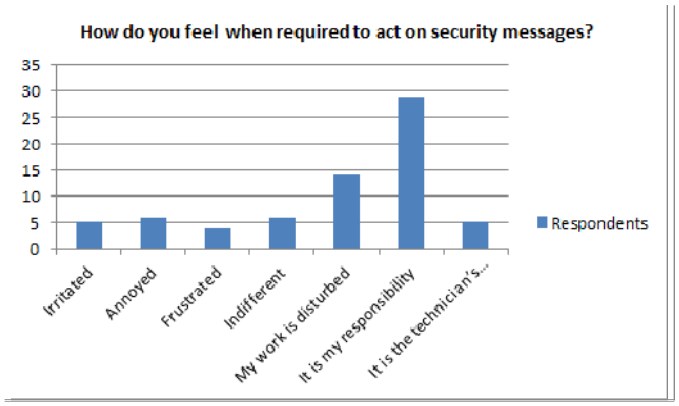


Figure 3: User feelings torwards acting on security messages

4. Security technology/Solution Usage

Anti-virus programs and passwords are the most used protection mechanisms with a prevalence of 72%, followed by firewalls. Updates are only implemented by 34% of respondents, which means that systems are left vulnerable to current and new attacks targeting known vulnerabilities. On further enquiry on users perform their updates, 70% of users identify with auto updates. The most shocking realisation is the fact that end users do not back up their information, with only 23% doing it.

The findings show that 46% of the participants configure security options. However, 68% are knowledgeable of the existence of spam filters in their email programs, possibly centrally configured for them by the system administrators. Other features such as encryption mechanisms for emails and files (digital signature, certificates same status) are rarely used. The security features interact with users through alerts, warnings and dialogue boxes in order to protect their information. A comparable survey carried out in 2006 also shows disturbing low usage of security technologies [12].

5. Embedded security feature knowledge

Only 46% of respondents have configured security options in their application programs. The idea of encrypting the information that is sent out via emails is virtually unknown, with only 4% using this feature. Embedded security is not being used as often as is necessary, and the absence thereof is making users an easy target for cybercriminals.

6. Behaviour towards security interactions

User behaviour is influenced by many factors such as lack of knowledge, prioritisation of their work targets and misconception of security threats [8]. The survey has confirmed the same facts. The majority of users make informed decisions (i.e. they actually read the screen before making a choice).

However, 18% ignore such information or just click in order to get rid of the message. When it comes to passwords, users seem to be more careful, although they are still susceptible to social engineering attacks. Users easily trust

anyone who claims to be technical support, with their login credentials (40% of respondents). They are cautious about email attachments, although they do trust emails from unknown sources.

When confronted with a computer problem, end users trust the insecure Internet (29% of respondents) for help, while 12.5% of respondents trust their colleagues to offer a solution. This exposes them to internal threats as well as to hackers. End users generally do not update their application programs as often as required with 27% of respondents doing it often, 53% when prompted by the software or technician, and 18.5% sometimes or never.

About 8% of respondents disable security programs from running on their PC and 17% disable alerts, but that the majority of respondents allow such application programs to run. Those who disable alerts do so because they feel negative about them. They feel irritated, annoyed, frustrated, or indifferent. Respondents also feel that their work is disrupted, or that it is the technician's responsibility to deal with security alerts. However, even among those who claim that it is their responsibility to look after security, there are some users who disable the alerts. This contradiction indicates that there is no alignment of behaviour to feelings (see Table 3).

There are mixed feelings about Web sensing, which manifests as a message that notifies the user that the page they are trying to access has been blocked by the organisation. Most respondents will navigate away from the site and do nothing about it. A few would contact the Webmaster. The patterns show that they are aware of restrictions to visit certain sites. If access to a genuine business related website is restricted, they act on it. However, the majority feels that it is appropriate for organisations to block some sites.

Another concern is the fact that many end users allow add-ons from the Internet to run on their computers, coupled with the fact that most of them have administrative rights (86% of respondents) on their machines. This poses a great security risk. Viruses and other malicious software can be executed remotely on their machines. Respondents download and install software from the Internet without making use of secure connections. Sixty per cent of respondents trust browser auto completion. This action might unknowingly lead them to a hacker's site.

7. Technology Acceptance

End users accept the use of a computer as a tool for accomplishing their daily tasks. However, they do not trust technicians with their information. Despite their comfort with technology they do not trust updates or new versions because it takes a lot of time to learn, because it moves them away from their comfort zone, or because of a fear of the unknown. However, some respondents are indifferent and will do as asked when prompted to update.

TABLE 3: FEELING ABOUT NOTIFICATIONS AND ERROR HANDLING

		Feelings about notifications						
		Irritated	Annoyed	Frustrated	Indifferent	Work is disturbed	My responsibility	Technician's responsibility
Alert Disabling	Yes	8	8	8	8	25	17	25
	No	7	9	5	9	19	47	4

C. Discussion

The results show that users are not trained with respect to security threats, solutions and secure behaviour while using information and communication technologies (ICT) to do their work. The organisation has policies in place to govern user behaviour with respect to ICT. However, end users have a low awareness of the existence of security policies and violate them by means of their behaviour. A large number of the participants download and install software programs from the Internet as they wish.

The results outlined above have several implications for Information Security. Considering the fact that all users have at least one computer connected to the Internet for their job, it is very important that all facets of Information Security [23] are addressed. However, due to lack of end user training, policies are violated exposing the participants to hacking attacks. End users (71% of respondents) download and install from the unsafe Internet. This can lead them to download malicious programs such as viruses, worms, Trojan horses, logic bombs and many others that will alter and destroy their information asset if executed. Since most users (87% of respondents) have administrative rights, it is quite easy for the compromised computers to be used to propagate the destruction of information in the organisation. The application programs that are most popularly used in the case site are rated as the most vulnerable by security experts [17]. This means that, with the human as the known weak link, attacks can be launched against the site via these application programs. There is evidence of poor information backup practices, with only 22% of respondents that are always performing this task. In the event of a cyber-attack, this would be very detrimental. Every computer has a super administrator password that is maintained by the technical team. However, when confronted with a problem, the participants give away their passwords to supposed helpdesk personnel. This is even done telephonically. This practice exposes users to social engineering attacks. In an academic institution a lot of sensitive information is at stake, including student records.

Poor security-related decisions and behaviour with an overall negative experience with Information Security are common, leaving application programs vulnerable to exploitation by cyber criminals.

VI. Recommendations

As interventions we recommend user training on computer security, ensuring that security policies are in place as well as the promotion of security-conscious behaviour.

Improving information security means improving the users' attitudes towards security features in the application programs that they use for their work. In order to improve the user experience with security features, users must be aware of security threats and solutions; they must know the benefits of using the features and must interact with the security features as required of them.

We recommend the UX model at Figure 1 with security awareness as the basis of feelings. Feelings shape attitudes and perceptions, which in turn influence behaviour. Negative behaviour with respect to security features will result in a negative experience with technology, and hence result in insecurity. This means that the user does not find the application programs usable for the job, resulting in information loss and/or compromise. Users will only be able to interact with embedded features if they feel good about it (the security will be usable).

VII. Conclusion

The research has highlighted problems that face end users while using computers to process, store and transmit personal or organisational information. The findings reflect a scenario in which there is a support mechanism from the organisation. It can be inferred that in scenarios where individuals are not supported, they experience more negative encounters with security. Based on the findings it is necessary to develop a framework for secure user experiences. The framework will ensure that users correctly interact while having a positive experience with built-in security features.

References

[1] Statistics, Internet World, Internet statistics usage : the Big picture. Inrernet WorldStats. Available http://www.internetworldstats.com/stats.htm , 2011.

[2] A. Herzog, & Shahmehri, N. User Help Techniques for usable security. ACM(1-59593-635-6/07/0003), 2007.

[3] A. Hanudin,, and T. Ramayah, (EJISDC (2010) 41, 2, 1-15). SMS banking: explaining the effects of attitude, social norms and perceived security and privacy. The Electronic Journal on Information Systems in Developing Countries 41(2), pp 1-15. Retrieved from http://www.ejisdc.org/ojs2/index.php/ejisdc/article/viewFile/638/315

[4] M. Cummings, Designing for interaction :*User experience. UX design What matters to interaction design Professionals*. CA, Silicon valley, USA: Uxmatters, 2008.

[5] ISO 9241-210. Ergonomics of Human System Interaction-Part 210, Human-Centred design for Interactive Systems, 2010.

[6] K. Schulze, and H. Krömker, A Framework to Measure User Experience of Interactive Online Products. *7th International Conference on Methods and Techniques in Behavioral Research*. Eindhoven, Netherlands: ACM. pp. 1-5, 2010.

[7] P. M. Desmet, and P. Hekkert, Framework of Product Experience. International Journal of Design, 1(1), pp. 57-66, 2007, March 30 .

[8] M. Hassenzahl and N. Tractinsky. User experience - a research agenda. Behaviour & Information Technology 25(2), 2006, March – April. pp. 91-97.

[9] L. F. Cranor, and S. Garfinkel, Security and usability: *Designing systems people can use*. Cambrige, USA: O'Reilly Media Inc, 2005.

[10] S. Furnell Usability versus complexity - striking the balance in end-user securityNetwork Security, 2010(12), pp. 13-17. doi:10.1016/s1353-4848 (10) 70147-1, 2010, December.

[11] P. Lew, L. Olsina, and L. Zhang, Integrating Quality, Quality in Use, Actual Usability and User Experience. 6th Central and Eastern European Software engineering Conference CEESECR. pp. 117-123,2010. Moscow, Russia: IEEE.

[12] S. M. Furnell, A. Jusoh, and D. Katsabas, The Challenges of understanding and using security: A survey of end-users, Computers and Security, 25, pp. 27-35, 2006.

[13] C. Giovanni, Top 10 Tools to Measure User Experience, 2012. Pragmatic Marketing, Inc.

[14] Nielsen Norman Group, Usability 101: Introduction to Usability, 2012, retrieved May 04,2012 from http://www.nngroup.com/articles/usability-101-introduction-to-usability/

[15] M. E. Whitman and H. Mattord, Principles of Information Security. USA: Thomson Course technology. 2011.

[16] A.Yeratziotis, D. van Greunen, and D. Pottas, Recommendations for Usable Security in Online Health Social Networks. IEEE. 978-1-45770208-2/11 pp. 220-226. 2011.

[17] SANS. Security prediction 2012 & 2013: The emerging security threat. SANS. Available http://www.sans.edu/research/security-laboratory/article/security-predict , 2011.

[18] R. K. Yin Case study Research : Design and Methods (4th ed., Vol. 5). London, UK: SAGE Inc.University Science, 2009.

[19] A. Bhattacherjee, Social Science Research:Principles, Methods, and Practices, 2nd ed. Florida: Global Text Project, 2012.

[20] I. Crinson and M. Leontowitsch, Public Health textbook: Qualitative methods. UK: PHAST (Public Health Action Support Team CIC). Retrieved from http://www.healthknowledge.org.uk/public-health-textbook/research-methods/1d-qualitative-methods , 2011.

[21] P. DePaulo, Sample size for qualitative research,. QUIRKS, 12, 2000.

[22] I. Dey, Qualitative data analysis: *A user-friendly guide for social scientists*, London: Taylor & Francis e-Library, 2005.

[23] M. Ciampa, Security+ Guide to Network Security Fundamentals, 3rd ed., Boston: Tomson Course Technology, 2011.

APPENDIX C2: CONFERENCE PAPER 2

Designing user security metrics for a security awareness at Higher and Tertiary Institutions

Fungai Bhunu Shava

Lecturer Polytechnic of Namibia

Windhoek, Namibia

Darelle Van Greunen

Nelson Mandela Metropolitan University

Port Elizabeth, South Africa

Abstract

Information security is at the heart of every organisation or individual who uses Information and Communication Technology (ICT) devices to socialize or for business. Security aims to ensure that users experience the three main goals of security: confidentiality, integrity and accountability (CIA). Despite the importance of security, very few organisations have proper plans to create awareness among their employees. Information security requires the user to be aware of the existence of security features on their electronic devices and to be able to use them appropriately. In a quest to establish the underlying reasons for increased exploitation despite the efforts in security solutions design, the focus is on awareness as a major factor influencing human behaviour. Online surveys were conducted to investigate security awareness levels in a case site. The case study was at an institution of higher and tertiary education in Namibia. Document review on security trends and approaches from selected leading industries was also done. Results show that most users are not aware of security policies operational in their organisation. In this paper we outline the security metrics that guide in formulating security awareness strategies.

Keywords

Security awareness, metrics, policy awareness

Introduction

Security awareness is the ability of a user to understand and implement security policies in programmes or organisations (Hubbard, 2002) According to Wilson and Hash (2003) awareness is meant to enable users to identify IT security concerns and to behave appropriately. Security depends mainly on user behaviour as most of the security actions depend on end user choices to act or not to act on security messages. To protect information and IT infrastructure the organisations need to have policies in place and to educate the users about them. Successful implementation and evaluation of security depends on the success of user education. NIST 8800-12 agrees that security responsibility awareness for users as well as training them on security best practices will change user behaviour (2007).

Most organisations have security policies; however, their users are not aware of the policies or the meaning and implications of implementing them. An extract from ISO/IEC17799:2005 section 8.2.2 on Information security awareness, education and training recommends that all end users ought to receive suitable awareness training and regular updates in organizational policies and procedures, as applicable to their job function.

Primarily, computer users log onto a computer system to communicate for social or business purposes, to share information and to get information from the World Wide Web. Among the people who communicate or share information or make information available for other users to download are cyber criminals. Cyber criminals capitalize on user behaviour when they access information on the web (2005).

Access to information has evolved and nowadays includes: the cloud and mobile devices of all sorts. To access information conveniently users tend to use removable devices (currently, usb devices), and multiple mobile devices. We argue that this provides convenience as the users are empowered to access their information always, anywhere. Furthermore, applications are designed to enhance the user interaction with technology. However, this convenience comes with a price as each device has its own inherent security weakness. Is the user aware of these weaknesses and of ways to protect themselves? The focus of this paper is to identify the main security threats which users should be aware of and to rank the risk they pose to the users. The importance of security policy, security awareness and human factors that can be used as metrics to enumerate the security in an organisation are discussed. The paper aims to answer a 3 research questions. The main research question is: How can the security metrics be used to come up with a security awareness strategy for a higher and tertiary institution? The research sub questions include:

What is the security awareness level among the case site community?
Which metrics can be used to measure the security awareness baseline?

This paper presents security metrics which can be used to evaluate the baseline security awareness of individual users before implementing awareness programs. The structure of the paper presents background information on information security awareness and security threats, objectives, methodology, findings, recommendations and conclusions.

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4Pages 280-296

Information Security Overview

The most important components of Information security are technology, process, policy and culture. ISO/IEC 27002 defines 12 security domains, namely: security policy, asset management, organizing information security, human resources, physical and environment, communication and operations management, access control, information system acquisition, development and maintenance, information security incident management, business continuity management and compliance. The 12 security domains are important when defining security metrics and coming up with security awareness strategies. We have borrowed from the domains in drawing up the security awareness metric that is the human resources component.

The importance of awareness cannot be ignored if security is a goal. Security awareness deals with the human resources security domain of the ISO/IEC 27002 guideline or code of practice. Furnell, Jusoh, and Katsabas (2005) made recommendations for improving user security, including user training on: application security and how best to use it, security threats one is exposed to when one connects to a network and how to manage those. Current research trends still allude to the fact that the human element is still the weakest link in InfoSec (Ernst & Young, 2014; Delloitte, 2013; SANS, 2013). The understanding of the human element could assist in defining the security metrics and awareness strategy. The Global Security survey by PWC (2014) confirms that the human aspect of security is the major risk. The same company in 2013 suggested three means that could be used to improve employee awareness as mentioned here:

- Attitudes and Perceptions - beliefs and opinions regarding the value and urgency of information security
- Behaviour - action taken to mitigate Information Security risk
- Knowledge, Skills and Abilities - insight into information security policies, procedures, and controls, roles/ responsibilities and business impact

Awareness, skills and abilities build perceptions and attitudes, which influence behavior and, in turn, consistent behavior can influence the overall security landscape for the organization. Figure 1 shows how these three factors influence the overall information security. Understanding the relationship of the human factors of InfoSec could help in the drawing up of the metric as it informs the relationship.

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4Pages 280-296

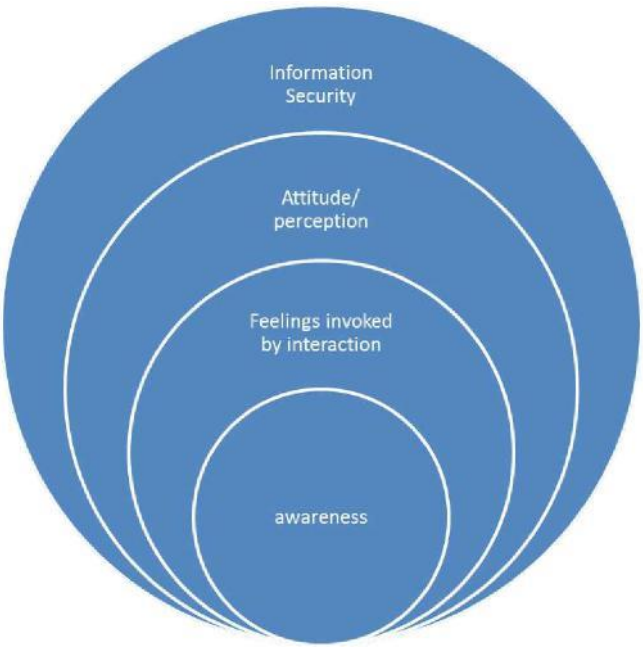


Figure 1: Security awareness impact on other security aspects

Security threats until 2016 have among them mobile devices as a way of penetrating enterprise security (Durbin, Steve; Olasvsrud, Thor, 2014). The reason for this is that: "the rapid development cycle and lack of security considerations around mobile apps make them a prime target for cybercriminals and hackers seeking a way into the enterprise" (Durbin, 2014). Nowadays, most people in the community can afford cell phones (smart phones, tablet PCs and other mobile devices) and as such, are bound to use them for e-commerce. Since the security on these devices is weak more hacktivism and malicious software will threaten InfoSec.

The Vision 2030 for Namibia has set a target to make available the latest, most affordable, modern and adequate ICT infrastructure to facilitate economic development and competiveness through innovation, research and development from the current level of 5.5 to 6.0 by 2017 (NDP4 page 77-8). The aim is to make Namibia a knowledge-based society by 2030 through reducing the digital divide between communities by ensuring the availability of broadband Internet in rural communities. NDP4: ICT provides fast access to information, which is a prerequisite for literacy and knowledge creation. These technologies are the modes of delivery for information economy (Government of Namibia, 2012).

Owing to affordability business processes will be conducted using smartphones or mobile devices (Durbin, 2014). These devices have a reputation of not being very secure, which presents an easier way for cyber criminals to get access into the enterprise by using them. The initiative to reduce the digital bridge and to enhance communication can also result in more InfoSec breaches. As the use of technology improves, precautions need to be taken to secure the beneficiaries.

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4Pages 280-296

Durbin and Olasvsrud (2014) recommend the incorporation of user devices into existing standards for access management, and that one should begin to promote education and awareness of BYOx (Bring Your Own Anything) risk in innovative ways.

Security Threats

An information security threat is an object that has potential to endanger information by exploiting vulnerabilities (Whitman & Mattord, 2011; Stallings, 2007). Table1 summarizes threats to InfoSec

Acts of human error or failure	Mistakes or accidents
Espionage or trespass	Unauthorized access or data collection
Information extortion	Blackmail or disclosure
Software attacks	Viruses, Denial of service (DoS)

Table 1: Common threats to InfoSec

If users are to protect themselves fully from these threats they need to be knowledgeable about them. A study carried out by Huang, Rau and Salvendy (2007) concluded that perceptions of information security threats could be described by means of six factors, namely: knowledge, impact, severity, controllability, possibility and awareness. Awareness is the beginning of knowledge. In order to educate users about security there is a need to raise their awareness first. The learning continuum presented by NIST 800-16 shows that awareness should be attained before training, as it prepares users for training by altering attitudes to realize the significance of security and the penalties of its failure (1998). It is therefore very important to address the root of the security challenges by ensuring that users are aware of threats before equipping them with the skills to protect themselves.

Security awareness trends

Security awareness refers to sharing information by educating and training users about risks to data, especially risks to the confidentiality, integrity, or availability of data, and about knowing what to do to protect data (Peltier, 2005), Companies worldwide are integrating security awareness programs in their business process to reduce the risk of losing information (PWC, 2014). Much has been said about how to measure the success of an awareness program; however, it is important for every organisation to identify their unique measures as well as other factors such as organizational culture and environmental influence awareness.

For effective evaluation of security risk, metrics for a security awareness baseline should be identified. According to Hayden (2010) “Security metrics should be about choosing the best methods to determine what you need to know about security so that you can understand and improve your operational processes, within the resource constraints you face” The research focuses on identifying metrics that can be used to measure the impact of security awareness on user behaviour and information security.

Awareness will empower users to make the right choices (Navarro, 2007). Security can be assessed by answering the following questions:

- Does the organization have security policies enforced?
- Do employees know the security policies?
- What are the practices and technologies in place that can help to detect a security breach?
- Do employees know what to do if they detect a security violation?

Ernst &Young carried out a survey in 2013 on emerging technologies and trends and found out that successful security needs improvement, expansion and innovation in awareness programs in order to foster more proactive behaviour than reactive behaviour among users. Their survey results showed that respondents were more confident in the capabilities of current technologies in use because they are familiar with and confident of their capabilities. Organisations were cited as tending to place more importance on current technology rather than on emerging or future trends. This leaves the organisations unprepared to cope with the rapid changes in the IT field, hence poor proactive awareness programs (Ernst & Young, 2013; PWC 2014).

In a similar study by PWC it was found that cloud computing and BYOD are being implemented before being secured (2014). Such strides in technology are driven by advanced technical people and, as such, it would be expected that such issues should not be there; however, human behaviour is always playing a pivotal role in the success of security. According to Gary Loveland, a new model of InfoSec, motivated by knowledge of threats, assets, and the motives and targets of potential adversaries, is necessary to address current security challenges (PWC, 2014). Since security implementation is through policies it is necessary to define what a policy is. The next section will focus on that.

Security Policies

“A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area.” (SANS, n.d.)

They are perceived as the main means by which organisations officially set out their position concerning information security activities (Brotby & Hinson, 2013).Properly implemented, policies can mitigate threats especially those that are due to human aspects. As they address user behaviour, it is therefore important that they are specific and understandable. Since policies are point specific, it means that an organisation can have several policies to address their diverse ICT needs.

Security awareness approach

Survey data collected from a case site was analysed qualitatively, based on the findings that emerged. According to Yin (2009); Bhattacherjee (2012); Crinson and Leontowitsch (2011) case study research is a detailed inquiry of an issue used to evaluate the authenticity of the problem and allows researchers to gather realistic data of the phenomenon being investigated in social and behavioral scientific research.

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4 Pages 280-296

Case site

A case study of the Polytechnic of Namibia (an academic institution in Namibia) was used for this paper. The Institution is located in the capital city of the nation, Windhoek. It has a student enrolment of 13400 per annum and employs 670 full-time staff. Every staff member has a desktop or personal computer (PC) and/or laptop allocated to him/her for daily work. The student laboratories and library are equipped with PCs, which are used for practical sessions as well as for information search on the internet and on e-library resources.

Materials and methods

A purposive, non-probabilistic method of sampling was used, targeting the sample population of staff members and aiming for a minimum of 30 responses.

Qualitative data analysis was used.

We therefore looked at the policing of and adherence to policies, as well as at security awareness.

The data gathered were classified according to exhibited patterns or characteristics, to allow for effective analysis. The classification was based on research aims and objectives. After classification of the data, we established connections among different categories.

The categories form the concepts or variables for the formulation of the theoretical framework, and for the relationships that form the connections. Meanings were logically inferred from literature. Description, contextualization, classification, processing and linking of gathered data were adopted.

Procedure

A survey was conducted in order to understand the security awareness levels in the case site. The population (site) was purposefully chosen to show the diversity of users from different backgrounds and professions, who use similar security features to achieve different outcomes. Purposive sampling is useful for circumstances where there is need to study a targeted sample in minimal time and proportion is not the key aspect. It is the most appropriate for selecting cases that are very informative (Saunders et al., 2009). Information about the knowledge of end users of the security threats to which they are exposed when they connect to networks; awareness of computer security policies in the organisation; and behaviour towards security alerts was gathered.

The objectives of the study were presented to the respondents in a cover letter. Based on this information, they made a voluntary informed choice whether or not to participate in the survey. Thus, purposive and self-selecting sampling techniques were used. Self-selection involves the participant volunteering to take part in the research and data was collected from those who responded. The responses were treated anonymously and in a confidential manner, to ensure that no link could be made to the participants who responded, on publishing the findings.

An online survey was designed to collect data from a population of about 670 end users using E-surveys Pro. The survey tool was pre-tested with seven users, after which it was deployed to all population members by means of a broadcast email containing the link. The online survey is quick and inexpensive to administer Furthermore; it saves time in analysis as the data can be analysed electronically using statistical tools.

Participant selection

The participants in this study comprised lecturers, administrators and other professionals who make up the university community. Participants were chosen for this qualitative experience evaluation because they possessed the common experience of avoiding the use of security features for one reason or the other. The institution has 670 full-time employees. The population was chosen in order to reflect a diversity of users from different backgrounds and professions, who use similar application programs for similar purposes to achieve different objectives. Students were not included as the study was aimed at reflecting on a typical work environment.

The respondent composition was representative of the university employee population and was spread across the different faculties and centers in the institution. Table 2 below presents the respondents' affiliations.

Department	Participants
School of Information Technology	18
School Of Business Management	8
School of Communication, Media & Legal Studies	2
School of Engineering	2
School of Natural resources	3
School of Health & Applied Sciences	1
Bureau of Computer Services	2
Centre of Open and Long life Learning	4
Centre of Teaching and learning	1
Centre of entrepreneurial development	1
Registrar	1
Library	1
Auxiliary Services	1
Payroll, Finance and Accounting	3
Human Resources	2
Namibian German Logistics	1
Security (Campus Control)	1

Table 2:Respondents affiliation

Data Analysis method

Responses from 53 participants who completed the survey out of 58 respondents were analysed for patterns that demonstrate how much the users think they know about information security. To gauge the security culture of the organisation, general security information was gathered. The information captured the understanding of security, threats and solutions, as well as whether the end users were implementing them or not. Then the

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa. ISBN: 978-0-620-63498-4 Pages 280-296

behaviour of end users with security feature/ technology and the reasons for the specific behaviour was assessed.

After this analysis, the results were used to develop security awareness metrics using the steps outlined in the next section. The data collected helped in understanding the security metrics required at PON.

Security metric program development process

Security metrics provide information about IT security including costs and risks (asset value, threat and vulnerability are elements of overall risk) and must be based on a rigorous approach for security measurements and applied understanding seeking information security (Hayden, 2010). Useful metrics reflect the degree to which security goals such as data confidentiality are being met and they drive actions taken to improve the overall security program of an organisation. They can also identify the risk levels of not implementing certain measures and can be used to raise the levels of awareness within the organisation (Payne, 2006).According to Hayden (2010) security is the result of human activity. Hence, in this study the focus was more on measuring the third element of risk-vulnerability. Facets of vulnerability include the degree of understanding of security issues among computer users. Based on the results presented in the previous section, metrics were developed using the Goal-Question method. For instance, the metric is policy awareness. The question asked is: to what extent do you know the following policies? The goal is to measure policy awareness level. The following are the 7 steps involved in developing a security metrics program and in this paper the focus was on the first three (Payne, 2006):

1. Define the metrics program objectives and goals (provide metrics that clearly communicate how user interaction with security can be improved. Goals: to base the metrics program on improving awareness within our organisation; to communicate effectively the metrics to all stake-holders, including end users)
2. Decide on which metrics to generate using either a framework, top-down or bottom-up approach to determine which metrics could be desirable to use. Start with goals, measurements to generate the metrics. The bottom up approach in Table 3 was adopted using the analysis of the survey results.

Bottom-Up Approach	
Identify measurements that can be collected for this process	% of people who are not aware of security policies in the organisation. % of people who are aware of security threats and solutions
Determine metrics that can be generated from the measurements	Train and improve the number of people aware of security policies, threats and solutions since last survey period.
Determine the association between derived metrics and established objectives of the overall security program	To increase security policy, threat and solution awareness among end users

Table 3: Bottom-up approach adopted from Payne(2006)

3. Develop strategies for generating the metrics (How will the data be collected?- Source (antivirus logs, user surveys), method of collection (survey, log analysis), frequency of collection, data analysis techniques, metric generation)
4. Establish the benchmarks and targets

5. Determine how the metrics will be reported
6. Create an action plan and act on it
7. Establish a formal program review/refinement cycle.

Findings and discussions

Security policies active in the organisation (Polytechnic of Namibia (PON)

The following policies exist in the case site:

1. Acceptable ICT use which is meant for all ICT users in the organisation. It is meant to spell out the tolerable use of computer equipment at PON to ensure that the infrastructure is protected from “risks including virus attacks, compromise of network systems and services, disclosure of confidential information and legal issues” (Polytecnic of Namibia, 2008).
2. Password Policy which defines a procedure for creating and protecting strong passwords, and the regularity of change.
3. Remote access, which is applicable to all users remotely accessing the PON network with either a PON-owned or personally-owned computer, laptop, workstation or Palm device. Used to connect to the PON network for work-related activities.
4. Virtual Private Network which specifies how to use Remote Access through IPsec or L2TP Virtual Private Network
5. (VPN) connections to the Polytechnic of Namibia (PON) corporate network.
6. Wireless communication which forbids connecting to the Polytechnic of Namibia (PON) networks through unsecured wireless communication mechanisms and stipulates that access can only be granted by the ICT department.

All these policies are really good, but does the implementation create the right atmosphere? Security policies are hardly known to the users, and therefore not used as shown in Table 4. Using risk factor assignment to questions; no knowledge of security policies presents a high risk factor for InfoSec and the higher the knowledge thereof the low the risk. Findings reflect:

To what extent do you know these policies? (1 is not at all and 5 is very well)

	12		3	4	5	Response Total
Password	11	2	11	12	15	51
Wireless	14	9	14	7	7	51
General computer usage	13	4	14	9	11	51
Internet	14	4	9	12	12	51

Table 4: Typical question

Response 1 is a very high risk factor (rated at 5) and 5 is the lowest risk factor (rated at 1). Generally the risk of policy knowledge is moderate to significant as the respondents are not knowledgeable of policies in the organization. According to practical lecturers and the technicians orally interviewed, students do not have enough storage on campus servers

and accessible PCs, coupled with the fact that their user accounts have mandatory user profiles. A mandatory user profile loses user information/data upon log off. This encourages the use of removable devices among staff and students as they share materials. Survey results reflect that 81of the respondents use memory sticks to share information. Memory sticks and email are the main means of sharing information. Other methods such as network, Google docs and Dropbox are just not popular. Emails and memory sticks are well known for propagating the spread of viruses. As a consequence of this, infections are rife in their labs and propagate to the production network. The anti-virus logs analysed show an infection rate of 85 virus infections in every hundred cases of malicious detections; the remainder being Trojan horses.

Security Policy awareness

A low policy awareness ranging between13% and 29% for the different policies is evident as presented in Figure 3. Figure 3 shows that of those who know about policies, 45% learnt about them from a colleague or friend. Some have never heard about the policies yet they use the policies very well.

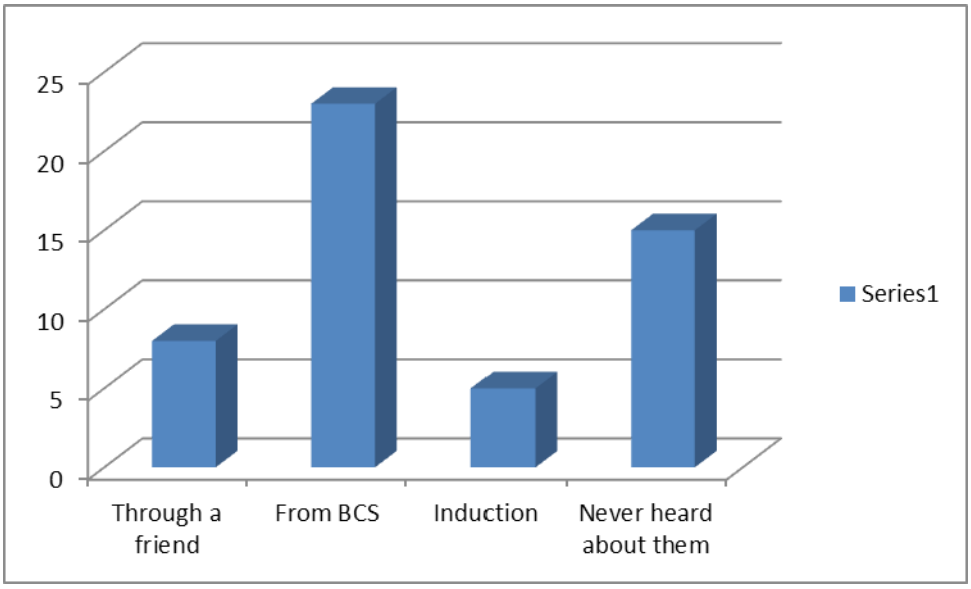


Figure 2: Where users learn about security policies

Users are generally not educated with regard to the existence of the policies, and they generally do learn about them from inappropriate sources. The findings reflect that there is no adherence to the policies as shown by the behaviour when confronted with a computer-related problem. The official way is to seek help from the Computer Services, yet about 42% seek it from the most untrusted source of information such as the Internet, or a friend or colleague. The general computer usage policy states that all sensitive information should be encrypted; yet the survey shows that only 15% of the respondents use the facility. This finding is a significant risk to information security.

Security Policy usage

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4 Pages 280-296

Of the 51 respondents, 31 (65%) know and follow the requirements of the policies as shown in Figure 4.

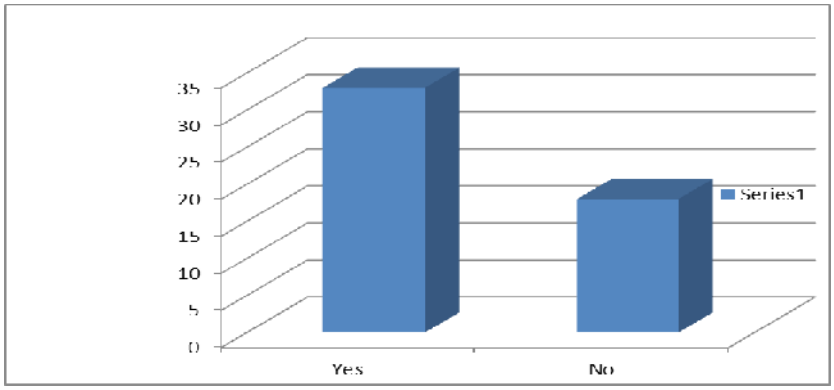


Figure 3: Knowledge of policy requirements

Section 4.2.2 of the Acceptable ICT use policy states that users must ensure the security of all passwords and that they are not to share accounts. The survey reveals that when confronted with a problem 40%, will disclose their passwords to the "support" personnel. The support can be offered telephonically or using remote desktop managers. They do not have any perception of the implications of disclosing their passwords. The risk associated with knowledge of policy requirements is moderate.

Security awareness levels at PON

There is no user to train users on information security as confirmed by 92% of the participants. However, some users are aware of some security aspects as shown by findings. Table 5 shows the responses from 53 participants to the question: Have you ever heard of the following? (Tick all that apply)

	Heard	%
Hacking	50	94
Phishing	45	85
Spam	49	92
Spyware	41	77
Virus	48	91
Worm	41	77
Social Engineering	16	30

Table 5: Knowledge of security threats

Generally, there is high security threat awareness even with no training. Using risk assignments, this shows that the security in the organisation is at low risk. Further enquiry shows that 23% of the same respondents do not know if they have been hacked or not, 57% do not know if they have been victims of social engineering as presented in Figure 5.

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4 Pages 280-296

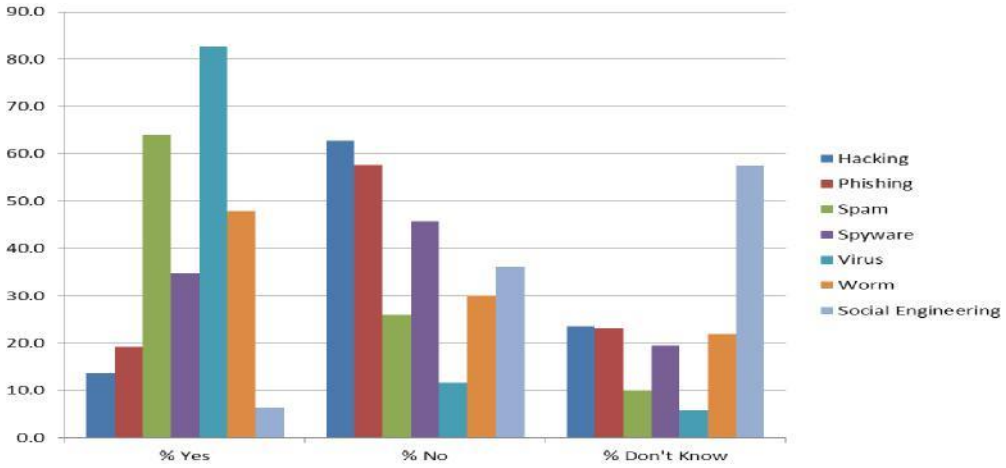


Figure 4: Have you been a victim of any of the threats?

End users (71%) download and install from the unsafe internet. This can lead them to download malicious programs such as viruses, worms, Trojan horses, logic bombs and many others, which will alter and destroy their information asset if executed. Since most (87%) have administrative rights it is quite easy for the compromised computers to be used to propagate the destruction of information in the organisation.

There is evidence of poor information backup practices, with only 22% performing the task always. In the event of a cyber-attack this will be very detrimental. Every computer has an administrator password which is maintained by the technical team. However, when confronted with a problem the participants give away their passwords to supposed helpdesk personnel, even telephonically. This practice exposes them to social engineering attacks. In an academic institution a lot is at stake, including student records. Summing up the findings there is moderate to significant risk posed by the awareness levels on information security.

Security metrics vs awareness

Based on the findings there is a need to develop and implement a security awareness program in the case site. Currently, the organisation is at level 1 of the security awareness roadmap depicted in figure 6.

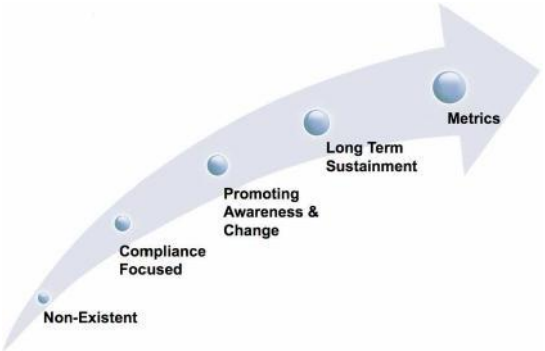


Figure 5: Security awareness roadmap adopted from SANS (2012)

The stages of implementing a security awareness program involve establishing a baseline, acting and then evaluating the impact. The security awareness metrics for establishing the baseline using the Goal-Question-Method presented in Table 6 is proposed:

Metric	What is measured	How it is measured	Details
Awareness survey	Number of users who: know about security policies, use policies, violate policies, know about security threats, breaches and solutions	Survey Tracking user behavior related to access policies	To what extend do users know/ understand or use security tools, features or policies?
User behavior	Number of users who behave negatively with security	Survey	What is the current status in the case site?
Computer infections	How many computers are infected?	Antivirus logs	Are the infections behavior related?

Table 6: Security awareness metrics

For one to be able to design effective security awareness there is a need to carry out an awareness survey to establish a baseline. The baseline will serve as a reference or comparison point for measuring the impact of awareness campaigns. It is important to know what computer users know already. The findings reflect the absence of user training. This is a direct measure of metric 1.The second metric from Table 6 is user behavior which should align to policy and best practices, the number of users behaving negatively can inform an organization on the need to draw up a security awareness plan. It is important to ant to have an understanding of what users do on the ICT resources. Thirdly, there is a need to know the computer attacks that affect the users, the frequency and how they impact on information and technology usage. Analysis of antivirus and system logs can reflect on the most prevalent infections, the sources, when it occurred and the number of devices affected. The source of infection and propagation mechanisms of breaches can inform what needs to be changed in terms of behavior and know-how.

Conclusion

The analysis of the collected data established that the policy awareness levels in the site were very low posing moderate to significant security risk for the case site. There is a need for a security awareness program to be designed and implemented especially addressing policy issues first since policies are the basis for defining best practices for human behavior with security-related issues. The awareness levels informed the identification of security metrics that can be used to establish the baseline state of security in a tertiary institution with security policies but no security awareness programs in place. This research identified what users need to be aware of namely security threats; policies and how to implement them in order to minimise the risk of vulnerability to information security threats; solutions and best practices. These are key indicators of the security risk levels.

The metrics extend existing work on security awareness by providing a measurement scheme for the first and second levels of the awareness roadmap. Information security officers can make informed decisions on areas of priority for the organisation and can thereby focus their programs on high priority areas first. The overall effectiveness of

Steyn, J., Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, held in Port Elizabeth, South Africa.ISBN: 978-0-620-63498-4 Pages 280-296

awareness intervention can be enumerated using suitable security awareness metrics after the implementation of the awareness program. In this paper it is argued that institutions of higher education can improve employee interaction with security features through security awareness programs which can be evaluated using well-defined security metrics as proposed. Security awareness, the number and frequency of computer infections as well as user behavior can be used to enumerate the baseline security in an environment. There is a need for developing a security awareness model that can be used to focus on critical security awareness aspects for improving user behavior with security. Future research will also focus on evaluating the applicability of these metrics to other environments other than academic instructions as security awareness is a global issue not confined to academia.

References

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices (2 edn.). Florida: Global Text Project.

Brotby, K. W., & Hinson, G. (2013). Pragmatic security metrics: applying metametrics to information security. Retrieved 2014, May 1from http://common.books24x7.com/toc.aspx?bookid=47301.

Crinson, I., & Leontowitsch, M. (2011). Public Health textbook: Qualitative methods. UK: PHAST (Public Health Action Support Team CIC). Retrieved August 4, 2012, from http://www.healthknowledge.org.uk/public-health-textbook/research-methods/1d-qualitative-methods

De Paulo, P. (2000). Sample size for qualitative research. QUIRKS, 12. Retrieved August 8, 2012, from http://www.quirks.com/articles/a2000/20001202.aspx?searchID=496600809

Dey, I. (2005). Qualitative data analysis: A user-friendly guide for social scientists. . London: Taylor & Francis e-Library. DOI: ISBN 0-203-72073-3

Furnell, S. M., Jusoh, A., & Katsabas, D. (2005). The Challenges of understanding and using security: A survey of end-users. Computers and Security, 25, 27-35. Retrieved January 24, 2012, from www.elsevier.com/locate/cose

Government of Namibia. (2012). Namibia's Fourth National Development Plan (NDP_4). Windhoek: Government of the republic of Namibia. Retrieved from npc.gov.na/ndp4

Hayden, L. (2010). IT security metrics: A practical framework for measuring security and protecting data. USA: McGraw-Hill.

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In J. A. Jacko, & J. A. Jacko (Ed.), Human-Computer Interaction. HCI Applications and Services (Vol. IV, pp. 906-915). Heidelberg: Springer.

ISO 9241-210. (2010). Ergonomics of Human System Interaction- Part 210, Human-Centred design for Interactive Systems. Retrieved September 28, 2012, from http://www.allaboutux.org/ux-definitions

ISO/IEC17799:2005. (2005). Information technology -- Security techniques -- Code of practice for information security management.

NIST. (1998). NIST SP 800-16 – Information Technology Security Training Requirements: A Role- and Performance-Based Model. USA.

Payne, S. C. (2006). A Guide to Security Metrics: SANS Security Essentials GSEC Practical Assignment Version 1.2e (2007). SANS.

Peltier, T. R. (2005). Implementing an information security awareness program. EDPACS, Vol 33(1), pp. 1-18.

Polytechnic of Namibia. (2008). Acceptable Use Policy.

Price Waterhouse Coopers. (2014). The Global State of Information Security Survey. United Kingdom: PWC. Retrieved 2014, June 17 from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

SANS. (2011). Security prediction 2012 & 2013 The emerging security threat. SANS. Retrieved February 24, 2012, from http://www.sans.edu/research/security-laboratory/article/security-predict2011

SANS. (n.d.). Information Security Policy Templates. Retrieved 2012, August 12 from http://www.sans.org/security-resources/policies/

Stallings, W. (2007). Network security Essentials: applications and standards (3rd edn.). New Jersey: Pearson International.

Whitman, M. E., & Mattord, H. (2011). Principles of Information Security. USA: Thomson Course technology.

Wilson, M., & Hash, J. (2003, October). Building an Information Technology Security Training and Awareness Program. NIST Special Publication 800-50, pp. 1-70.

Yin, R. K. (2009). Case Study Research: Design and Methods (4th edn, Vol. 5). London, UK: SAGE Inc.

APPENDIX C3: BOOK CHAPTER

CHAPTER TEN

DEVELOPING USER SECURITY METRICS TOWARDS AWARENESS CREATION

FUNGAI BHUNU SHAVA

DARELLE VAN GREUNEN

Introduction

Developing countries are currently experiencing a transformation in the use of Information Technology (IT). These countries are adopting ICT and greatly increasing their use of ICT and the Internet. They have expectations for the positive impact of their investment, but it is not always clear what the level of security awareness is amongst the end users. Developing countries are emerging ICT nations and their populations are emerging online. Such users are often perceived as easy targets as they have limited security awareness in the digital environment.

Security awareness refers to the extent to which a user can understand and implement security policies in programs or organizations (Hubbard 2002). According to Wilson and Hash (2003), awareness empowers users to identify IT security concerns and to behave appropriately. Security occurs as a result of user behavior as most of the security actions depend on end user choices to act or not to act on security messages. To protect information and IT infrastructure the organizations need to design and implement policies as well as to educate users about them. Successful implementation and evaluation of security depends on the success of user education. According to the NIST 800-12 special publication, user security responsibility awareness as well as security best practice training can enhance secure user behavior (NIST 1995:143).

Most organizations have security policies; however, their users are not aware of the policies or the meaning and implications of implementing them. An extract from ISO/IEC17799: 2005 Section 8.2.2 on information security awareness, education and training recommends that all end users should receive suitable awareness training and regular updates in organizational policies and procedures, as applicable to their job function.
Primarily, computer users log on to a computer system to socialize or conduct business, to share information and to access information from the World Wide Web. Among the people who participate in information communication or sharing or making information available for other users to download are cyber criminals. Cyber criminals always capitalize on user actions online to launch their attacks.
Access to information is continuously evolving and currently includes: the cloud and mobile devices of all sorts (Internet of Things). For convenient information access, storage and sharing users tend to use removable devices (currently, USB devices), and multiple mobile devices. We argue that this provides convenience as the users are empowered to access their information always, anywhere. Furthermore, applications are designed to enhance the user interaction with such technology. However, this convenience comes with risks as each device has its peculiar inherent security weakness. Are the users cognizant of these weaknesses and of means to protect themselves? The motivation of this chapter is to identify the main security threats that users ought to be conscious of and to rank the risks they pose to the users. The significance of security policy, security awareness and human factors that can be used to enumerate the security posture in an organization is discussed. The goals of security center on the security triad: confidentiality, integrity and availability. This chapter aims to answer three research questions. The main research question is: How can security metrics be used to come up with a security awareness strategy for a higher or tertiary institution in a developing country? The research sub-questions include:

- What is the security awareness level among the case site community in a typical developing country?
- Which metrics can be used to measure the security awareness baseline?

This chapter examines the adoption of end user security features by developing nations that are rapidly deploying information and

communication technologies. It studied a higher education institution in Namibia to draw lessons of the situation and potential methods of improving the situation. Based on the findings, security metrics are presented that can be used to evaluate the baseline security awareness of individual users in a developing country context before implementing awareness programs. The structure of the chapter presents background information on information security awareness and security threats, objectives, methodology, findings, recommendations and conclusions.

Information Security Overview

The most important comments with regard to information security are: technology, process, policy and culture (Guyot 2003). ISO/IEC 27002 defines 12 security domains, namely: risk assessment, security policy, asset management, organizing information security, human resources, physical and environment, communication and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management and compliance.

The latest version is the ISO27002: 2013 with 14 domains. The new domains are cryptography and supplier relationships, and the existing domain communications and operations management were divided into two domains, namely operations and communications security (ISO/IEC 2013). The security domains are vital when outlining security metrics and coming up with security awareness strategies. We have focused on the human resources security to be able to draw up the security awareness metrics.

The importance of awareness cannot be ignored if security is a goal. Security awareness deals with the human resources security domain of the ISO/IEC 27002 guideline or code of practice. Furnell, Jusoh and Katsabas (2005) made recommendations for improving user security, including user training on: application security and how best to use it, security threats one is exposed to when one connects to a network, and how to manage those. Current research trends allude to the fact that the human element is still the weakest link in InfoSec (Ernst and Young 2013; Deloitte 2013; SANS 2013). The understanding of the human element could assist in defining the security metrics and awareness strategy. The Global Security survey

by PWC (2014) confirms that the human aspect of security is its major risk. The same company in 2013 suggested three ways that could be used to improve employee awareness:

- Attitudes and Perceptions - beliefs and opinions regarding the
- value and urgency of information security
- Behavior - action taken to mitigate information security risk
- Knowledge, Skills and Abilities - insight into information
- security policies, procedures, and controls, roles/ responsibilities and business impact.

The link among these three ways is shown in Figure 10-1. Awareness is the basis of knowledge, skills and abilities. These, in turn, build perceptions and attitudes, which influence behavior. Security conscious behavior and choices can be influenced through awareness strategies targeting security related education (Kajzer et al. 2014). Consistent positive behavior can impact the overall security landscape for the organization in the right direction.

[Figure 10-1. How to influence user behavior]

Figure 10-2 shows how these three factors influence overall information security. Understanding the relationship of the human factors of InfoSec could help in the drawing up of the metric as it informs the relationship.

[Figure 10-2. Security awareness impact on other security aspects]

Security threats predictions until the year 2016 had among them mobile devices as a way of penetrating enterprise security (Durbin and Olasvsrud 2014). The reason for this was attributed to that fact that mobile applications are hurriedly developed without security considerations hence they are targeted as an entry point in enterprises (Durbin 2013). Nowadays, most people in the community can afford cell phones (smart phones, tablet PCs and other mobile devices) and as such, are most likely to use them for e-commerce. Since the security on these devices is weak, more hacktivism and malicious software will continue to threaten InfoSec.

Vision 2030 for Namibia has set a target to make available the latest, most affordable, modern and adequate ICT infrastructure to facilitate economic

development and competiveness through innovation, research and development from the current level of 5.5 to 6.0 by 2017 (NDP4 2012:77-78). The aim is to make Namibia a knowledge-based society by 2030 through reducing the digital divide between communities by ensuring the availability of broadband Internet in rural communities. Namibia Development Plan 4 (NDP4): ICT provides fast access to information, which is a prerequisite for literacy and knowledge creation. These technologies are the modes of delivery for information economy (Government of Namibia 2012).

Owing to affordability, business processes will be conducted using smartphones or mobile devices (Durbin and Olasvsrud 2014). These devices have a reputation of not being very secure, which presents an easier way for cyber criminals to get access into the enterprise by using them. The initiative to reduce the digital bridge and to enhance communication can also result in more InfoSec breaches. As the use of technology improves, precautions need to be taken to secure its beneficiaries.

Durbin and Olasvsrud (2014) recommend the incorporation of user devices into existing standards for access management, and that one should begin to promote education and awareness of BYOx (Bring Your Own Anything) risk in innovative ways.

Security Threats

An information security threat is an object that has the potential to endanger information by exploiting vulnerabilities (Whitman and Mattord 2011; Stallings 2007). Threats to InfoSec can be classified either as acts of human error or failure, or as mistakes/accidents as summarized in Table 10-1.

Acts of human error or failure	Mistakes or accidents
Espionage or trespass	Unauthorized access or data collection
Information extortion	Blackmail or disclosure
Software attacks	Viruses, Denial of service (DoS)

Table 10-1. Security threats

For users to protect themselves from these threats they should be educated about them. Perceptions of information security threats can be defined by using the following six factors, namely: knowledge, impact, severity, controllability, possibility and awareness (Huang, Rau and Salvendy 2007). Knowledge originates from awareness. As such, user awareness of security should be addressed first if users are to be educated regarding security. The NIST 800-16 (1998) learning continuum begins with awareness before training, as a way of getting the user ready for training by shifting attitudes to recognizing the importance of security and the consequences of its failure. For a secure organization, it is vital to ensure user awareness of security threats and challenges before providing them with the skills to defend themselves.

Security awareness trends

Security awareness encompasses sharing information through instructing and teaching users about risks to data and information, focusing on risks to confidentiality, integrity, or availability of data, and knowledge of actions to use in order to protect data (Peltier 2005). The global trend is for companies to incorporate security awareness programs in their business process to reduce the risk of information loss (PWC 2014). Much effort has been directed to measuring the success of awareness programs; however, every organization has unique measures influenced by its organizational culture and by environmental influences on security awareness.

Metrics for a security awareness reference point need to be known to enable effective assessment of security risk. According to Hayden (2010, 27) "Security metrics should be about choosing the best methods to determine what you need to know about security so that you can understand and improve your operational processes, within the resource constraints you face". In this chapter, emphasis is on identifying metrics that can be used to measure the impact of security awareness on user behavior and information security.

According to Navarro (2007) security awareness will empower users to make the right choices. Security can be assessed by answering the following questions:

- Does the organization have enforced security policies?
- Do employees know the security policies?

- What are the practices and technologies in place that can help to detect a
- security breach?
- Do employees know what to do if they detect a security violation?

Ernst and Young (2013) carried out a survey on emerging technologies and trends and found out that successful security needs improvement, expansion and innovation in awareness programs in order to foster more proactive behavior than reactive behavior among users. Their survey results showed that respondents were more confident in the capabilities of current technologies in use because they are familiar with and confident of their capabilities. Organizations were cited as tending to place more importance on current technology rather than on emerging or future trends. This leaves the organizations unprepared to cope with the rapid changes in the IT field, hence poor proactive awareness programs (Ernst and Young 2013; PWC 2014).

In a similar study by PWC (2014), it was found that cloud computing and BYOD are being implemented before being secured. Such strides in technology are driven by advanced technical people and, as such, it would be expected that such issues should not be there; however, human behavior always plays a pivotal role in the success of security. According to Gary Loveland, a new model of InfoSec, motivated by knowledge of threats, assets, and the motives and targets of potential adversaries, is necessary to address current security challenges (PWC 2014). Since security implementation is achieved through policies, it is necessary to define what a policy is. The next section will focus on that.

Security Policies

"A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area." (SANS n.d.).

Policies are perceived to be the foremost way for organizations to define their stance on information security activities formally (Brotby and Hinson 2013). If implemented appropriately, policies can mitigate threats resultant from human aspects. Policies deal with user behavior; as such they must be specific and understandable. As policies are point specific, an

organization can have several policies, each focusing on one element of their varied ICT needs.

Security awareness approach

According to (Spitzner, Lance 2012), if no awareness program is in place then the focus should first be placed on compliance, which addresses the implementation of standards, promoting user awareness and change through an awareness program tailored for the organizational needs; on long-term sustainment, which addresses how to improve the organizational posture continually through unceasing improvement; and on metrics, which measure the effectiveness of the awareness program. Survey data collected from a case site was analyzed qualitatively. Based on the findings that emerged, security metrics were proposed. According to Yin (2009); Bhattacherjee (2012); as well as Crinson and Leontowitsch (2011), case study research is the detailed inquiry of an issue used to evaluate the authenticity of the problem and it allows researchers to gather realistic data of the phenomenon being investigated in social and behavioral scientific research.

Case site

A case study of the Polytechnic of Namibia (an academic institution in Namibia) was conducted. The Institution is located in the capital city of the nation, Windhoek. It has a student enrolment of 13'400 and employs 670 full-time staff. Every staff member has a desktop or personal computer (PC) and/or laptop allocated to him/her for daily work. The student laboratories and library are equipped with PCs used for practical sessions as well as for information search on the Internet and on e-library resources.

Materials and methods

Using a purposive, non-probabilistic method of sampling, the aim was to receive a minimum of 30 responses from the target population of staff members. We considered the policing of and adherence to policies, as well as at security awareness.

To allow for effective analysis, the data classification was implemented according to exhibited patterns or characteristics. The classification

focused on research aims and objectives. After classification of the data, connections were established among different categories. The categories form the concepts or variables for the formulation of the theoretical framework, and for the relationships that form the connections. Meanings were logically inferred from literature. Description, contextualization, classification, processing and linking of gathered data were adopted.

Procedure

A survey was conducted in order to understand the security awareness levels in the case site. The population (site) was purposefully chosen to show the diversity of users from different backgrounds and professions, who use similar security features to achieve different outcomes. Purposive sampling is useful for circumstances where there is a need to study a targeted sample in minimal time and where proportion is not the key aspect. It is most appropriate for selecting cases that are very informative (Saunders et al. 2009). Information was gathered regarding the knowledge of end users of the security threats to which they are exposed when they connect to networks; awareness of computer security policies in the organization; and behavior towards security alerts.

The objectives of the study were presented to the respondents in a covering letter. Based on this information, they made a voluntary informed choice whether or not to participate in the survey. Thus, purposive and self-selecting sampling techniques were used. Self-selection involves the participant volunteering to take part in the research. Data was collected from those who responded. The responses were treated anonymously and in a confidential manner, to ensure that no link could be made to the participants who responded, on publication of the findings.

An online survey was designed to collect data from a population of about 670 end users using E-surveys Pro. The survey tool was pre-tested with seven users, after which it was deployed to all population members by means of a broadcast email containing the link. The online survey is quick and inexpensive to administer. Furthermore, it saves time in analysis as the data can be analyzed electronically using statistical tools.

Participant selection

The participants in this study comprised lecturers, administrators and other professionals who make up the university community. Participants were chosen for this qualitative experience evaluation because they possessed the common experience of avoiding the use of security features for one reason or another. The institution has 670 full-time employees. The population was chosen in order to reflect a diversity of users from different backgrounds and professions, who use similar application programs for similar purposes in order to achieve different objectives. Students were not included as the study was aimed at reflecting on a typical work environment.

The respondent composition was representative of the university employee population and was spread across the different faculties and centers in the institution. Table 10-2 below presents the affiliations of the respondents.

Department	Participants
School of Information Technology	18
School of Business Management	8
School of Communication, Media and Legal Studies	2
School of Engineering	2
School of Natural Resources	3
School of Health and Applied Sciences	1
Bureau of Computer Services	2
Centre of Open and Long Life Learning	4
Centre of Teaching and Learning	1
Centre of Entrepreneurial Development	1
Registrar	1
Library	1
Auxiliary Services	1
Payroll, Finance and Accounting	3
Human Resources	2
Namibian German Logistics	1
Security (Campus Control)	1

Table 10-2. Affiliations of respondents

Data Analysis method

Responses from 53 participants who completed the survey out of 58 respondents were analyzed for patterns that demonstrate how much the users think they know about information security. To gauge the security culture of the organization, general security information was gathered. The information captured the understanding of security, threats and solutions, as well as whether the end users were implementing them or not. Then the behavior of end users was assessed with security feature/ technology and the reasons for the specific behavior.

After this analysis, the results were used to develop security awareness metrics using the steps outlined in the next section. The data collected helped in understanding the security metrics required at the case site.

Security metric development process

Security metrics provide information about IT security, including costs and risks (asset value, threat and vulnerability are elements of overall risk), and must be based on a rigorous approach for security measurements and applied understanding seeking information security (Hayden 2010). Worthwhile metrics reflect the degree to which security goals are being achieved and they motivate actions taken to advance the security program of an organization. They can also pinpoint the risk levels of not implementing certain actions and can be used to improve the levels of awareness within the organization (Payne 2006). According to Hayden (2010), security occurs as a result of human activity. This study focused on measuring the human element of risk- vulnerability. Dimensions of vulnerability include the level of understanding of security concerns by computer users. Based on the results presented in the previous section, metrics were developed using the Goal-Question method. For instance, the metric is user behavior. The question asked is: how do you behave when confronted with a security dialogue? The goal is to measure user behavior with security dialogue boxes. The following are the seven steps involved in developing a security metrics program. In this chapter the focus was on the first three (Payne 2006):

1. Define the metrics program objectives and goals (provide metrics that clearly communicate how user interaction with security can be improved. Goals: to base the metrics program on improving awareness within our organization; to communicate effectively the metrics to all stake-holders, including end users).

2. Decide on metrics to be produced by means of a framework, top-down or bottom-up approach and identify metrics which would be appropriate to use. First, define the goals; then come up with measurements to generate the metrics. The bottom-up approach as described by Payne (2006) in Table 10-3 was adopted after analyzing the survey results.
3. Develop strategies for generating the metrics (How will the data be collected and how often? - Source (antivirus logs, user surveys), method of collection (survey, log analysis), frequency of collection, data analysis techniques, metric generation).
4. Establish benchmarks and targets.
5. Decide how the metrics will be reported.
6. Make an action plan and implement it.
7. Establish a formal program review/refinement cycle.

Bottom-Up Approach	
Identify measurements that can be collected for this process	The percentage of users unaware of security policies in the organization; security threats and solutions; the ratio of users who behave securely
Define metrics that can be generated from the measurements	The number of users knowledgeable of security policies; threats and solutions from the last dated survey; people who behave securely and successful security breaches recorded in logs.
Determine the association between resulting metrics and established objectives of the overall security program	To increase security policy, threat and solution awareness among end users

Table 10-3. Bottom-up approach employed for analysis of results

Findings and discussions

Security policies active in the organization

The analysis of documentation at the case site revealed a list of policies for implementation. The following policies exist in the case site:

1. Acceptable ICT use describes the acceptable use of ICT equipment in the institution to guarantee that the organization is safe from "risks including virus attacks, compromise of network systems and services, disclosure of confidential information and legal issues" which is meant for all ICT users in the organization. It is meant to spell out acceptable use of ICT resources (Polytechnic of Namibia, 2008).
2. Password Policy defining practice for constructing and safe guarding strong passwords, and the frequency of change.

3. Remote access, for all employees accessing the institution's network off-campus with either a company-owned or personal computer, laptop, workstation or mobile device for work-related activities.
4. Virtual Private Network (VPN) which prescribes how to use Remote Access through IPsec or L2TP VPN connections to the organization's corporate network.
5. Wireless communication that prohibits connecting to the organization's networks through unsafe mobile communication devices and specifies that access can only be approved by the ICT department.

The policies are well articulated; however, the effect of their implementation on user experience is unknown. Users barely know the security policies; hence, they do not use them as expected. Table 10-4 shows the usage statistics from the survey data answering the question: "To what extent do you know these policies? (1 is not at all and 5 is very well)"

	1	2	3	4	5	Response Total
Password	11	2	11	12	15	51
Wireless	14	9	14	7	7	51
General Computer usage	13	4	14	9	11	51
Internet	14	4	9	12	12	51

Table 10-4. Knowledge of policies

Extent 1 shows a significant risk rated at five (5), and Extent 5 is the least risk rated at one (1). In general, the risk of policy knowledge is moderate (3.04) as the participants have average to low knowledge of policies in the organization. Computer practical lectures and computer laboratory technicians who were orally interviewed alluded that students are not allocated enough memory on campus servers and end user PCs, and they have mandatory user accounts. A mandatory user profile does not store user information/data when they log off. This promotes the use of removable devices among computer users as they share and save materials. From the survey results, 81% of the respondents use memory sticks for information sharing, after emails. Other methods of information

sharing such as network, Google docs and DropBox are just not popular. Emails and memory sticks are well known to be good vectors for distributing viruses. As a result of this, malicious code is a significant problem in computer laboratories and extends to the staff network. Anti-virus logs show a virus infection rate of 85 in every hundred cases of detections; 15 out of 100 are Trojan horses.

Using risk factor assignment to questions where no knowledge of security policies presents a high risk factor for InfoSec and the higher the knowledge thereof the lower the risk. Table 15-5 shows the calculated awareness risk value for various policies in the organization.

Policy	Average risk value	Awareness risk value	Risk rating
Password	171/51= 3.35	50	Elevated
Wireless	137/51=2.69	40	Elevated
General Computer Usage	154/51=3.02	45	Elevated
Internet	157/51= 3.08	46	Elevated
Overall	3.04	45	Elevated

Table 15-5. Calculated risk rating for security policy awareness

Security Policy awareness

Policy awareness as low as 13% to a slightly higher 29% for the different policies is indicated in the results. Figure 10-3 shows how those knowledgeable about policies learnt about them. Interestingly, among those who responded some were not aware of the policies, yet they responded positively on usage.

[Figure 10-3. Where users learn about security policies]

There is a need for user education with regard to policy existence, to ensure that those who know about them have learnt from correct sources. The findings show that there is no compliance to policies as reflected by user behavior when challenged with computer issues. The procedural way to respond is to find assistance from the respective department; however, about 42% source help from unsecure sources, including Internet, friends or colleagues. According to the general computer usage policy, all sensitive information must be encrypted. The reality is that as few as 15% of the respondents use the facility. The status quo poses a significant risk to the organizational security.

Security Policy usage

Of the 51 respondents, 31 (65%) know and follow the requirements of the policies as shown in Figure 10-4. Others claim to know about policies but do not follow the requirements.

[Figure 10-4. Knowledge of policy requirements]

Section 4.2.2 of the Acceptable ICT use policy speaks about the responsibility of users regarding password security and account sharing. However, survey findings show that when confronted with a problem, 40% will share their passwords with the "support" personnel. The support can be telephonic or remote using remote desktop managers. Users do not have an understanding of the implications of sharing their passwords. The risk associated with knowledge of policy requirements is average.

Security awareness levels in the organization

There is no user training on information security as reported by 92% of the respondents. However, some users know some security aspects as reflected in the findings. Table 15-6 shows the responses from 53 participants to the question: "Have you ever heard of the following? (Tick all that apply)".

	Heard of	%	Risk level
Hacking	50	94	14
Phishing	45	85	13
Spam	49	92	14
Spyware	41	77	12
Virus	48	91	14
Worm	41	77	12
Social Engineering	16	30	45
Overall			18

Table 15-6. Knowledge of security threats and associated risk rating

Table 15-6 shows a significant level of security threat awareness except on social engineering, despite users being untrained. Using risk calculations, the security risk of the organization is low. However responses to other

related questions show that 23% of the same respondents do not know if they have been victims of hacking or not, while 57% do not know if they have been socially engineered as shown in Figure 15-5.

[Figure 15-5. Victims of security threats]

User behavior influences the overall security status of an organization. As part of the survey, we gathered information on security interaction behavior. When presented with a security dialogue, the majority of users actually read the message before clicking on an option, except for 18% who disregard the message and select options as a way of removing the dialogue box. Password security is high; however, they are vulnerable to social engineering attacks as 40% of respondents, easily trust technical support staff with their login credentials. Email security behavior is good, but can still be improved regarding handling emails from unknown sources.

Technical help source poses a moderate risk, as 29% of respondents seek advice from the Internet and 12.5% from their colleagues. Software updates are rarely done as reflected in Table 15-7. This can open backdoors for cyber-attacks. End users have a tendency to allow add-ons from the Internet to execute on their machines. All these actions for users with administrative rights (87% of respondents) are a significant risk and need to be addressed. This also explains the high manifestations of viruses and other malicious software.

	Not at all	**Rarely**	**Sometimes**	**Often**	**Always**	**Response Total**
Antivirus	1	0	6	8	38	53
Firewall	6	4	6	11	26	53
Antimalware	25	7	6	5	10	53
Intrusion Detection System	28	8	8	4	5	53
Passwords	3	0	3	9	38	53
Patches	25	7	7	4	10	53
Updates	5	7	9	14	18	53
Backup	5	5	17	14	12	53
Encryption	24	12	7	6	4	53

Table 15-7. Frequency of use of specific security technologies

There is low information backup awareness. The study showed that only 22% always perform it. The organization has moderate to significant risk posed by the awareness levels on information security behavior.

Security metrics vs awareness

Based on the findings, there is a need to develop and implement a security awareness program in the case site. Currently, the organization is at level 1 of the security awareness roadmap as described by SANS (2012). The security awareness roadmap has different levels with the first level stated as non-existent, followed by compliance focused. The third level speaks to promoting awareness and change that in turn leads to long term sustainment that results in metrics at the final level 5.

The stages of implementing a security awareness program involve establishing a baseline, acting and then evaluating the impact. Based on the findings, we propose specific security awareness metrics for establishing the baseline (see Table 15-8). We used the Goal-Question-Method to derive the metrics.

Metric	What is measured?	How it is measured	Details
Awareness survey	Number of users who: know about security policies; use policies; violate policies; know about security threats, breaches and solutions	Survey Tracking user behavior related to access policies	To what extent do users know/ understand or use security tools, features or policies?
User behavior	Number of users who behave negatively with security	Survey	What is the current status at the case site?
Computer infections	How many computers are infected?	Antivirus logs	Are the infections behavior related?

Table 15-8. Security awareness metrics

For one to be able to design effective security awareness there is a need to carry out an awareness survey to establish a baseline. The baseline will serve as a reference or comparison point for measuring the impact of awareness campaigns. It is important to know what computer users know already. The findings reflect the absence of user training. This is a direct measure of metric 1.

The second metric from Table 15-8 is user behavior, which should align to policy and best practices. The number of users behaving negatively can inform an organization of the need to draw up a security awareness plan. It is important to have an understanding of what users do with the ICT resources. Thirdly, there is a need to know the computer attacks that affect the users, their frequency and how these impact information and technology usage. Analysis of antivirus and system logs can reflect on the most prevalent infections, the sources, when they occurred and the number of devices affected. The source of infection and the propagation mechanisms of breaches can inform what needs to be changed in terms of behavior and know-how.

Conclusion

The findings of the study show that policy and secure behavior awareness levels in the site are very low, presenting moderate to significant security threats for the organization. There is a need for a security awareness program to be designed and implemented not only in the developed world but also in the emerging countries. Such programs should target policy and secure behavior first and foremost. Policies form the foundation for security implementation and they define the rules and procedure of how end users should behave as well as the associated consequences of policy violation. Based on the awareness levels, security metrics for establishing the security baseline in the tertiary institution were identified. These can now be used by similar institutions in developing countries to determine the level of security awareness within different establishments.

The findings indicated that the institution has good security policies, but no security awareness programs in place. This research identified what end users need to be aware of, namely: security threats; policies and procedures of implementation as a way of reducing the risk of cyber-

attacks; solutions and best practices. The identified metrics are crucial pointers to security risk levels. The study outputs (metrics) extend the body of knowledge on security awareness by proposing a measurement scheme for levels 1 and 2 of the security awareness roadmap by SANS (2012). The metrics will enable security officers to make informed decisions to focus on priority areas of organizational security.

The overall value of awareness mediation can be calculated using suitable security awareness metrics after implementing a suitable awareness program. In this study we argue that tertiary education institutions can improve information security postures by influencing user behavior with security features through tailored security awareness programs. The awareness programs are assessed using the proposed security metrics. Baseline security can be assessed using user awareness of security issues, threats and solution; the amount and rate of occurrence of computer infections; and user behavior.

This study found that policy makers in developing countries need better guidance on how to create awareness amongst their end users. There is a need for a better understanding of the security challenges in those nations. The challenges faced need to be better articulated and the situation analyzed for ways to respond to the challenges and where further research is needed. This study contributed towards a security awareness model that focuses on critical security awareness aspects for improving user behavior with security. Future research will focus on evaluating the applicability of these metrics to non-academic institutions in Namibia.

References

Bhattacherjee, Anol. (2012). Social Science Research:Principles, Methods, and Practices. 2. Florida: Global Text Project.

Brotby, Kraig W, and Hinson , Gary. (2013). Pragmatic security metrics: applying metametrics to information security. New York: Auerbach Publications.

Crinson, I, and M Leontowitsch. (2011). Public Health textbook: Qualitative methods. UK: PHAST (Public Health Action Support Team CIC).

Deloitte. (2013). Blurring the Lines Information security in a world without boundaries. Deloitte Touche Tohmatsu Limited.
Durbin, Steve. (2013). Threat Horizon 2015 - Executive Summary. *Threat Horizon 2015 - Executive Summary*. Information Security Forum, January 31, 2013.
Durbin, Steve; Olasvsrud, Thor. (2014). Threat Horizon 2014. *Information Security Forum*.
Ernst and Young. (2013). Insights on governance, risk and compliance-Under cyber attack: EY's global information security survey 2013. Ernst and Young, 1-28.
Furnell, Steven, M, Jusoh, Adila, and Katsabas, Dimitris. (2005). The Challenges of understanding and using security: A survey of end-users. *Computers and Security*, 25: 27-35.
Furnell, Steven. (2010). Usability versus complexity - striking the balance in end-user security. *Network Security* 12: 13-17.
Government of Namibia. (2012). Namibia's Fourth National Development Plan (NDP_4). Windhoek: Government of the republic of Namibia.
Guyot, Lloyd. (2003). Essential information security for corporate employees: The most essential best practices. SANS Institute.
Hayden, Lance. (2010). IT security metrics: A practical framework for measuring security and protecting data. USA: McGraw-Hill. 27.
Huang, Ding-Long, Rau, Pei-Luen Patrick and Salvendy, Gavriel. (2007). A survey of factors influencing people's perception of information security. Vol. IV, in Human-Computer Interaction. HCI Applications and Services, by Julie A. Jacko, edited by Julie, A. Jacko, 906-915. Heidelberg: Springer.
Hubbard, William. (2002). Methods and Techniques of Implementing a Security: GSEC Practical Assignment, version 1.3. SANS.
ISO/IEC. *ISO/IEC 27002:2013(E).* Standard, ISO/IEC. (2013).
ISO/IEC17799:2005. (2005). Information technology -- Security techniques -- Code of practice for information security management.
Kajzer, Mitchell, John D'Arcy, Charles R. Crowell, and Dirk Van Bruggen. (2014). An exploratory investigation of message person congruence in information security awareness campaigns. *Computers and Security*, 43: 64 - 76.
Navarro, Luis. (2007). Train employees - your best defense - for security awareness. *SC magazine*, February 21, 2007.

NIST. (1995). An introduction to computer security: the NIST handbook. NIST special publication 800-12. Edited by Barbara Guttman and Edward A Roback. NIST. USA, October 1995.

NIST. (2003). NIST SP 800-16 – Information Technology Security Training Requirements: A Role- and Performance-Based Model. USA, 1998. Building an Information Technology Security Training and Awareness Program. NIST Special Publication 800-50, October 2003: 1-70.

Payne, Shirley C. (2006). A Guide to Security Metrics: SANS Security Essentials GSEC Practical Assignment Version 1.2e (2007). SANS.

Peltier, Thomas R. (2005). Implementing an information security awareness program." Security Management Practices (Information Systems Security), May/June: 37-49.

Price Waterhouse Coopers (PWC). (2014). The Global State of Information Security Survey. UK: Price Waterhouse Coopers.

SANS. (n.d.). Information Security Policy Templates.

SANS. (2011). Security prediction 2012 and 2013 The emerging security threat. Security trends, SANS.

Saunders, Mark, Philip Lewis, and Adrian Thornhill. (2009). Research Methods for Business Students. 5th . England: Pearson Education Limited.

Spitzner, Lance. (2012). Security awareness maturity model promoting change. SANS.

Spitzner, Lance. (2012). Next generation security awareness programs: securing the human. SANS.

Stallings, William. (2007). Network security Essentials: applications ans standards. 3rd . New Jersey: Pearson International.

Whitman, Michael, E and Mattord, Herbert, J. (2011). Principles of Information Security. USA: Thomson Course technology.

Wilson , Mark, and Joan Hash. (2003). Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50. Washington: NIST, October 2003.

Yin, Robert K. (2009). Case study Research : Design and Methods. 4th . Vol. 5. London: SAGE Inc.

APPENDIX C4: EDITOR'S LETTER

RICKY WOODS
Proofreading and Editing

26 December 2015

Prof. Darelle van Greunen

Nelson Mandela Metropolitan University

Dear Madam

Proofreading of Doctoral Thesis

I, Marietjie Alfreda Woods, hereby certify that I have completed the proofreading and correction of the thesis, **A Framework to Evaluate User Experience of End User Application Security Features** by **Fungai Bhunu Shava**, submitted in fulfilment of the requirements for the degree **Philosophiae Doctor** in **Information Technology** in the **Faculty of Engineering, the Built Environment and Information Technology** at the **Nelson Mandela Metropolitan University**

My own credentials are as follows: I completed reading for a BA degree in 1977 at the University of the Witwatersrand, majoring in English and Afrikaans en Nederlands. Thereafter, I completed a Higher Education Diploma. I have been teaching English Home Language since 1979

I am currently Head of Department Languages at Alexander Road High School, where I have been Subject Head of English for the past fourteen years. I have also been working formally in the area of editing and proofreading online since the beginning of 2011. I have accreditation in Copy-Editing and Proofreading from the South African Writers' College.

I believe that the thesis meets with the grammatical and linguistic requirements for a document of this nature.

Yours faithfully

(Mrs) M.A.Woods, BA, HDE (PG) (Wits), BA (Hons) (Psych), Dip Sp Ed (Unisa)

10 Framesby Plein, Sandra Avenue, Framesby, Port Elizabeth, 6045, Tel. 041-360 8763, 083 3126310