UNIVERSITY *of the*
WESTERN CAPE

A FUNCTIONAL-INTERPRETIVE APPROACH TO INFORMATION SYSTEMS SECURITY E-COMPETENCIES DEVELOPMENT IN THE HIGHER EDUCATION INSTITUTION: A COMPARATIVE CASE OF FOUR SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS

A thesis submitted in fulfilment of the requirements for the Doctoral degree in

INFORMATION SYSTEMS

In the

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

OF THE UNIVERSITY OF THE WESTERN CAPE

by

Mukenge Simon – Tshinu

Supervisor: Dr Zoran Mitrovic

March 2016

DECLARATION

I, Mukenge Simon Tshinu hereby declare that this thesis, which is submitted for the PhD in Information Systems to the University of Western Cape and titled **A FUNCTIONAL-INTERPRETIVE APPROACH TO INFORMATION SYSTEMS SECURITY E-COMPETENCIES DEVELOPMENT IN THE HIGHER EDUCATION INSTITUTION: A COMPARATIVE CASE OF FOUR SOUTH AFRICAN HIGHER EDUCATION INSTITUTIONS** is my original work and has not been previously submitted to any other university for the awarding of any academic qualification. The sources quoted are acknowledged by giving credit to the author or authors through referencing and complete bibliography.

Mukenge Simon Tshinu

---------- ----------

Signature Date: March 2016

ACKNOWLEDGEMENTS

My sincere appreciation to the men, women and institutions that have supported me and/or advised me in any form throughout the research process without which the study could not have successfully been completed.

My appreciation goes to my supervisor, Dr Zoran Mitrovic for his advice, intellectual and moral support to me from our first interaction to the day of submission of this research. I also offer my gratitude to Dr Michael Twum Darko and Elmari Snoer who contributed greatly to this research by proofreading the draft.

My appreciation goes to our Dean of Faculty of Business and Management Sciences, Professor Mzikayise S. Binza, for his understanding and timely approval of all my requests related to this research, his moral support that stimulated me to complete this research. At the same time I wish to thank the Cape Peninsula University of Technology (CPUT) for its financial support provided during my studies.

Likewise, I am grateful to the ICT security experts and respondents from various HEIs in South Africa and their respective institutions for their time sacrificed to participate in this research through interviews and the completion of questionnaires.

Finally I am thankful for the good understanding and support from my wife Deborah Bondo, my children Esther Tshinu and Piet-Smith Tshinu, my parents, brothers and sisters for bearing the time while I completed this research.

To you all who have assisted me during the completion of this research, I thank you.

DEDICATION

This research report is dedicated to my father Tshinu Mukendi Mathieu who without losing patience provided for my education and imparted a sense of perseverance in me. I wish he could live and rejoice together with us in this great achievement.

To God be the glory for the great things he has done.

ABSTRACT

Higher Education Institutions (HEIs) in this current age of modernisation rely on Information and Communication Technology (ICT) resources of various forms to process information that support their business decisions, conduct research, to engage in teaching and learning, and to communicate with various stakeholders across their different campuses and the entire world.

To be helpful and produce reliable information, the ICT systems and Information Systems (IS) resources in general need to be protected against all forms of internal and external threats. Also essential is the protection against the intentional and unintentional threats that can affect the confidentiality, integrity, and availability criteria of information and related information systems resources.

In this regard, information and related information resources like Information and Communication Technology (ICT) has become core to the operations of HEIs and is now increasingly pervasive. Also, employees in the HEIs now use them for work related activities both on and off campus. The literature reports that the protection of information and related IS resources has become a responsibility of every end user in the HEI environment rather than the few ICT technicians and their security technologies. It follows that every end user needs to be provided with proper IS security e-competencies to ensure effective protection of the organisational IS resources they access. This responsibility has now become a legal prerequisite for every organisation (including HEIs) that collects, processes, and stores their customers' information.

There are existing IT or ICT competency frameworks such as Skills Framework for Information Age (SFIA), and the European e-Competence Framework (e-CF) that are available to measure the skills of only professional IT people working in the IT industry. However, these frameworks accommodate only the IS security competencies at higher level end users in the Higher Education Institution (HEI) environment.

The research reported in this thesis examines the approaches of four (4) HEIs in the Western Cape Province in South Africa to institutional development of IS security e-competencies across their full staff compliments. It used a mixed research methodology and multiple case study research design in which four Higher Education Institutions (HEIs) participated. A total of 26 in-depth interviews were conducted and 385 questionnaires were completed. The research found that these HEIs do not formally develop the IS security e-competencies of their IS resources end users. Because end users handle critical information and research projects of importance not only to the HEIs, but also to the country, this situation creates a potential risk to their IS resources. In other words, the HEIs that participated in this research rely more on the ICT security technology itself to protect their IS resources than on the human side of ICT security. This is in direct contrast to the established literature which clearly points out that it is the internal end users that pose the most threats to IS security resources and these threats are more dangerous than the external threats.

As a result, this research proposes an IS security e-competencies development framework that classifies the end users in the HEI environment, identifies required IS security e-competencies for end users, and proposes the appropriate methods for delivering these identified security e-competencies. The proposed IS security e-competencies framework can be integrated into the existing HEI strategies for ICT security, and can also be used as an inventory tool for end users' IS security e-competencies development.

Keywords: ICT Security, e-Competencies, Knowledge, Skills, Attitudes, Information and Communication Technology (ICT), Competency Frameworks, Higher Education Institution (HEI), ICT policies, Training and development.

TABLE OF CONTENTS

DECLARATION ..... **I**
ACKNOWLEDGEMENTS ..... **II**
DEDICATION ..... **III**
ABSTRACT ..... **IV**
TABLE OF CONTENTS ..... **VI**
LIST OF FIGURES ..... **XII**
LIST OF TABLES ..... **XIII**
LIST OF ABBREVIATIONS ..... **XV**

CHAPTER ONE: INTRODUCTION AND BACKGROUND **1**
1.1 INTRODUCTION 1
1.2 DISCUSSING THE CONCEPTS 2
1.2.1 Information Technology (IT), Information Systems (IS), and Information and Communication Technology (ICT) *3*
1.2.2 Information Systems security *4*
1.2.3 Competencies and IS security e-competencies *5*
1.2.4 IS resources end users *5*
1.2.5 Higher education institution (HEI) *5*
1.3 BACKGROUND AND RESEARCH PROBLEM STATEMENT 6
1.4 AIM AND OBJECTIVES OF THE STUDY 10
1.4.1 Research objectives *10*
1.4.2 Research sub-objectives *11*
1.5 RESEARCH QUESTION AND SUB-QUESTIONS 12
1.5.1 Research sub-questions *12*
1.6 OVERVIEW OF RESEARCH DESIGN AND METHODOLOGY 14
1.6.1 Research method and strategy *14*
1.6.2 Overview of the underlying theory *16*
1.6.3 Research assumptions *17*
1.6.3 Ethical considerations *18*
1.7 BRIEF FINDINGS FROM THE STUDY 19
1.7.1 Brief findings from the literature *19*

1.7.2 Brief findings from the empirical study *21*
1.8 CONTRIBUTION OF THIS STUDY 22
1.9 RESEARCH DELIMITATION 22
1.10 THESIS OUTLINE 23
1.11 CHAPTER SUMMARY 25

CHAPTER TWO: UNDERLYING RESEARCH THEORY 27
2.1 INTRODUCTION 27
2.2 GENERAL PERSPECTIVE OF THEORIES IN RESEARCH 27
2.3 PERSPECTIVE ON ACTIVITY THEORY 28
2.3.1 Historical background of Activity Theory 29
2.3.2 Components of Activity Theory 30
2.3.3 Principles of Activity Theory 35
2.3.4 Motivation for applying Activity Theory in IS security e-competencies development 36
2.3.5 Applying Activity Theory in other learning contexts 40
2.4 CHAPTER SUMMARY 42

CHAPTER THREE: LITERATURE REVIEW – CONTEXTUALISING IS RESOURCES IN THE HIGHER EDUCATION CONTEXT 43
3.1 INTRODUCTION 43
3.2 COMMON INFORMATION SYSTEMS (IS) RESOURCES AND THEIR SECURITY CRITERIA 44
3.2.1 Common Information Systems resources 44
3.2.2 Information and Information Systems resources criteria 47
3.3 INFORMATION SYSTEMS – THREATS AND SECURITY MEASURES 49
3.3.1 Common sources of threats to Information Systems 50
3.4 ICT SECURITY MODEL AND STANDARDS 55
3.4.1 The IS security defense-in-depth model 55
3.4.2 The International Organisation for Standardisation – ISO 27001 and ISO 27002 57
3.5 LITERATURE REVIEW ON IS RESOURCES SECURITY 64
3.6 IS RESOURCES SECURITY AND ORGANISATIONAL CULTURE 67

3.7 IS RESOURCES SECURITY AND LEGAL REQUIREMENTS 70
3.8.4 IS resources security e-competencies development and legal implication (Acts) in Higher Education (HE) environment 72
3.8 IS SECURITY E-COMPETENCIES DEVELOPMENT AND THE TOP MANAGEMENT AGENDA: THE ISSUE OF GOVERNANCE 73
3.9 CHAPTER SUMMARY 75

CHAPTER FOUR: LITERATURE REVIEW – EXISTING FRAMEWORKS ON IS SECURITY E-COMPETENCY DEVELOPMENT AND THEIR CONTEXT IN HIGHER EDUCATION INSTITUTION 77
4.1 INTRODUCTION 77
4.2 TERMS AND DEFINITIONS 78
4.2.1 Knowledge and IS security e-competencies 81
4.2.2 Skills and IS security e-competencies 82
4.2.3 Ability and IS security e-competencies 82
4.2.4 Behaviour and IS security e-competencies 83
4.3 INFORMATION SYSTEMS SECURITY E-COMPETENCY AND IS SECURITY 86
4.4 IMPORTANCE OF SECURITY E-COMPETENCIES IN HEI 88
4.5 GENERAL FRAMEWORKS ON COMPETENCIES 89
4.5.1 IS security e-competencies with reference to Skills Framework for Information Age (SFIA) 90
4.5.2 The European e-Competence Framework (e-CF) 92
4.6 DEVELOPING A FRAMEWORK FOR END USERS IS SECURITY E-COMPETENCIES DEVELOPMENT 96
4.7 PREVIOUS RESEARCHES ON IS COMPETENCIES 100
4.7.1 Competencies in other industries 100
4.7.2 Competencies in other IS related fields 101
4.8 DEVELOPING IS SECURITY E-COMPETENCIES IN HIGHER EDUCATION 102
4.8.1 Training, awareness programme, and education 103
4.8.2 Training and awareness programme costs and benefits 104
4.8.3 Kim and Park model for competency-based training 106

4.8.4 The triple A competency model as training model 108
4.8.5 Training and development from IS and security related fields 110
4.9 CHAPTER SUMMARY 114

CHAPTER FIVE: RESEARCH DESIGN AND METHODOLOGY 116
5.1 INTRODUCTION 116
5.2 RESEARCH DESIGN 116
5.3 PHILOSOPHICAL APPROACH OF THIS RESEARCH 118
5.3.1 Philosophical perspectives 118
5.3.2 Research paradigms described 120
5.3.3 This study and research paradigm 123
5.4 POPULATION AND THE SAMPLE 128
5.4.1 Population and the study sample 129
5.4.2 Sampling tools and techniques 131
5.5 TECHNIQUES FOR DATA COLLETION AND ANALYSIS 134
5.5.1 Data collection techniques 135
5.5.2 Data analysis techniques 139
5.6 DATA VALIDITY AND SECURITY 142
5.7 CHAPTER SUMMARY 143

CHAPTER SIX: DATA ANALYSIS 145
6.1 INTRODUCTION 145
6.2 INTERACTION WITH EXPERTS ON IS SECURITY E-COMPETENCIES 146
6.2.1 Experts' views on IS security e-competencies development: Object or purpose component of Activity Theory (AT) 146
6.3 ANALYSIS OF DATA FROM THE FOUR PARTICIPATING HEIS 153
6.3.1 Presentation of cases (Include the participating HEIs) 153
6.3.2 Analysing data collected from the four participating HEIs 153
6.4 CHAPTER SUMMARY 205

CHAPTER SEVEN: FINDINGS AND DISCUSSION 207
7.1 INTRODUCTION 207

7.2 EMPIRICAL JUSTIFICATION OF THE STUDY FROM THE PRACTITIONERS PERSPECTIVE 207
7.3 SUMMARY OF THE FINDING 209
7.3.1 Sub-objective 1: The analysis of the importance of IS resources and their security in the HEI environment 209
7.3.2 Sub-objective 2: The exploration of IS security e-competencies development practices as practiced by the four participating HEIs 212
7.3.3 Sub-objective 3: Summary of data from the exploration of optimal ways of supplying the needed IS security e-competencies in the HE environment 217
7.4 IS E-COMPETENCIES DEVELOPMENT OVERARCHING ACTIVITY SYSTEM (OAS) 224
7.5 THE IS SECURITY E-COMPETENCIES DEVELOPMENT FRAMEWORK ... 228
7.5.1 Management support and strategic direction 232
7.5.2 The best practice frameworks and legal requirements 233
7.5.3 Classification of information (and other infrastructure) 233
7.5.4 End user levels of IS security e-competencies 235
7.5.5 IS security e-competencies 236
7.5.6 Methods of supplying the IS security e-competencies 236
7.6 IMPORTANCE OF THE SOLUTION 239
7.7 JUSTIFICATION OF RESEARCH FINDINGS 240
7.8 CHAPTER SUMMARY 242

CHAPTER EIGHT: CONCLUSION AND RECOMMENDATIONS 244
8.1 INTRODUCTION 244
8.2 MEETING RESEARCH OBJECTIVES 244
8.3 OVERVIEW OF LITERATURE REVIEW 246
8.4 OVERVIEW OF EMPIRICAL RESEARCH DESIGN 247
8.5 SUMMARY OF DATA ANALYSIS AND RESULTS 248
8.6 CONTRIBUTIONS OF THE STUDY 249
8.7 LIMITATIONS OF THE STUDY 252
8.8 RECOMMENDATIONS 253
8.8.1 University Council and executive leadership on IS security e-competencies development 254

8.8.2 IS security e-competencies practices and ICT security policy 254
8.8.3 The challenge in the supply of IS security e-competencies 255
8.8.4 The supply of IS security e-competencies 255
8.8.5 The use of ICT security framework 256
8.9 RECOMMENDATIONS FOR FUTURE RESEARCH 256
8.10 CHAPTER SUMMARY 257

REFERENCES 260

APPENDICES 295
APPENDIX A: UWC ETHICAL CLEARANCE 295
APPENDIX B: STEPS FOR DESIGNING A COMPETENCY FRAMEWORK 297
APPENDIX C: QUANTITATIVE DATA ANALYSIS RESEARCH CODE BOOK IN SPSS 298
APPENDIX D: SOUTH AFRICAN INFORMATION SECURITY ACTS 302
APPENDIX E: PARTICIPANTS PROFILE AND RESPONSE RATE 309
APPENDIX F: PARTICIPANTS' QUOTATIONS AND VIEWS ON CHALLENGES EXPERIENCED THAT PREVENT THEM FROM DEVELOPING END USERS IS SECURITY E-COMPETENCIES .. 315
APPENDIX G: PARTICIPANTS' QUOTATIONS AND VIEWS ON IS SECURITY THREATS FACED IN THEIR RESPECTIVE HEIS 317
APPENDIX H: EXPERT VIEWS AND QUOTATIONS ON THE OBJECT OF IS SECURITY E-COMPETENCIES DEVELOPMENT 319
APPENDIX I: PARTICIPANTS' VIEWS ON THE IMPORTANCE OF ICT RESOURCES IN THE HEI ENVIRONMENT 320
APPENDIX J: PARTICIPANTS' VIEWS ON THE CRITICAL ICT SYSTEMS IN THEIR INSTITUTIONS 321
APPENDIX K: PARTICIPANTS' VIEWS ON THE IS SECURITY E-COMPETENCIES DEVELOPMENT IN THEIR INSTITUTIONS 322
APPENDIX L: PARTICIPANTS' VIEWS ON THE IDENTIFICATION AND CATEGORISATION OF CRITICAL IS RESOURCES END USERS IN THEIR INSTITUTIONS 323
APPENDIX M: PARTICIPANTS' VIEWS ON THE TRAINING CHALLENGES IN GENERAL 324
APPENDIX N: PARTICIPANTS' VIEWS ON THE APPROACHES TO TRAINING 325

LIST OF FIGURES

Figure 1.1: Theoretical framework based on the activity system 16
Figure 2.1: First generation of Activity Theory 29
Figure 2.2: The IS security e-competencies development conceptualisation as Overarching Activity System (OAS) 39
Figure 3.1: Effect of people security e-competency on other IS resources 46
Figure 3.2: IS security defense-in-depth model 56
Figure 3.3: ICT Security Management System (ISMS) process model 63
Figure 3.4: Organisational and end users security culture and policy bond 68
Figure 4.1: Competency-based training steps 107
Figure 4.2: The triple A Competency model 110
Figure 5.1: Research population and sample 130
Figure 7.1: IS security e-competency development OAS 224
Figure 7.2: IS Security e-competencies development framework for end users 230

LIST OF TABLES

Table 3.1: Summary of threats to IS resources and related security measures 54
Table 6.1: Experts and university of affiliation 146
Table 6.2: Experts' views on the importance of security training for end users in the protection of IS resources? 148
Table 6.3: Experts' view of the importance of a security policy for the protection of IS resources? 148
Table 6.4: Experts' view of the importance of the security culture important for the protection of IS resources? 148
Table 6.5: Content of ICT security e-competencies development 149
*Table 6.6: Participants' dependability on computer and other IT resources to do their work * Higher Education Institution (HEI) Reference Cross tabulation 157*
*Table 6.7: Participants' dependability on own computer or mobile phone to access e-mails and connect to network off the campus * Higher Education Institution (HEI) Reference Cross tabulation 158*
Table 6.8: Chi-Square Tests 159
*Table 6.9: Participants' view on their responsibility towards IT resources security * Higher Education Institution (HEI) Reference Cross tabulation 160*
Table 6.10: Chi-Square Tests 161
*Table 6.11: End users' views on attendance of formal training on IT security at their institution? * Higher Education Institution (HEI) Reference Cross tabulation 165*
Table 6.12: Chi-Square Tests 166
*Table 6.13: Place of IT security training * Higher Education Institution (HEI) Reference Cross tabulation 167*
Table 6.14: Frequency table: End users' ability to identify different security threats affecting IT resources they have accessed in their environment 173
*Table 6.15: End users' ability to identify different security threats affecting IT resources they have accessed in their environment * Higher Education Institution (HEI) Reference Cross tabulation 174*
Table 6.16: Chi-Square Tests 175
Table 6.17: Frequency table: the relevancy of the IT security competencies towards the end users' work 182

Table 6.18: Statistics - the relevancy of the IT security competencies towards the end users' work *182*
*Table 6.19: The relevancy of the IT security competencies towards the end users' work * Higher Education Institution (HEI) Reference Cross tabulation* *183*
Table 6.20: Chi-Square Tests *184*
Table 6.21: Statistics – End users' knowledge of the legal implications of their actions on IT resources and related security *188*
Table 6.22: Frequencies – End users' knowledge of the legal implications of their actions on IT resources and related security *188*
*Table 6.23: End users' knowledge of the legal implications of their actions on IT resources and related security * Higher Education Institution (HEI) Reference Cross tabulation* *189*
Table 6.24: Chi-Square Tests *190*
Table 6.25: End users' willingness to attend institutional IT security training related to their job level *195*
*Table 6.26: End users' willingness to attend institutional IT security training related to their job level * Higher Education Institution (HEI) Reference Cross tabulation* *196*
Table 6.27: Chi-Square Tests *196*
Table 6.28: End users' preference towards classroom (contact) mode *197*
Table 6.29: End users' preference towards online training mode *198*
Table 6.30: End users' preference towards information provided on CD or DVD ... *198*
Table 6.31: End users' preference towards printed notes for self-reading? *198*
Table 7.1: Spheres of IS security e-competencies content *208*

LIST OF ABBREVIATIONS

AT = Activity Theory

CBT = Computer-based training

CD = Compact Discs

COBIT = Control Objectives for Information and Related Technology

CPNI = Centre for the Protection of National Infrastructure

DVD = Digital Video Discs

e-CF = European e-Competencies Framework

ECT = Electronic Communications and Transaction act

e-HR = Electronic Human Resource

HCT = Human Capital Theory

HEI = Higher Education Institution

HEQF = Higher Education Qualification Framework

HRIS = Human Resource Information System

IA = Information Assurance

ICT = Information and Communication Technology

INCOSE = International Council on Systems Engineering

IRMA = Information Resources Management Association

IRSE = Institution of Railway Signal Engineers

IS = Information Systems

ISMS = ICT Security Management System

ISO = International Organisation for Standardisation

IT = Information Technology

ITS = Integrated Tertiary System

NIAC = National Infrastructure Advisory Council

PAI = Promotion of Access to Information act

POPI = Protection of Personal Information act

RACI = Responsibility, Accountability, Consulted, and Informed

SFIA = Skills Framework for the Information Age

UWC = University of Western Cape

WBT = Web-based training

CHAPTER ONE: INTRODUCTION AND BACKGROUND

This chapter presents an overview of the research at hand as well as its importance on Information Systems (IS) security e-competencies development framework. The research applies Activity Theory (AT) as theoretical lenses in the process of understanding the importance of information systems (IS) resources security e-competencies in the Higher Education (HE) environment. The AT also forms the plan for the research and applies special attention to the research problem, aims, sub-questions and methodology.

1.1 INTRODUCTION

The security of Information and Communication Technology (ICT) resources in any organisation (including Higher Education Institutions - HEIs) is a well-established issue known for many years. Recently, it has been amplified due to the increased reliance on ICT resources (Whitman & Mattord, 2010:2; Jones, 2009). According to Jones (2009), previously information security was more about locks, bars and valuable documents to be stored in safes and filing cabinets with security guards executing physical checks. Still, there were cases of security breaches that resulted from carelessness of employees with the organisational information and communication technologies (ICT) resources and printed documents. Today, the rapid escalation in the number and form of threats has brought another dimension in the protection of valuable IS resources.

The accelerated innovation in the ICT field, especially the Internet and remote transactions processing (Gollmann, 2011:6-11; Gourova et *al*., 2009), the increased adoption of IS resources (Avison & Pries-Heje, 2005:193) and increased investment in ICT with expectation of improved efficiency and competitiveness (Piccoli, 2012:26-27; Yoon, 2009b) by many modern organisations and HEIs have impacted how organisations approach the security of their ICT resources. This has brought challenges and security threats (Gollmann, 2011:23) which are dynamic and evolving as technology evolves (Furnell, 2009) and this requires a pragmatic and integrated approach to ICT security management.

The case for IS security e-competencies across the full staff compliment in the HEI context is very: real because ICT security threats are increasingly occurring and evolving. However, the matter is complex because the activity involves knowledge of both threats and security measures. It involves various stakeholders with different tasks to perform and different skills, as well as involving the application of both technological and non-technological control measures. Further, Organisations are faced with different types of losses that range from financial the loss of credibility, legal cases and fines and possible imprisonment.

Thus, a careful approach to building IS security e-competencies is required in order to prevent or alleviate threats and also to resolve complex IS security and IS security e-competencies development issues.

1.2 DISCUSSING THE CONCEPTS

Before engaging in more detailed discussion of the other aspects of this research, it is important to discuss some of the common concepts that are used in this research. This is done in order to avoid possible misinterpretation and confusion of terms as some concepts are used to express ideas which maybe in contrast to their everyday use.

It is also important at this point to note that IS is a fairly new field of study (Pries-Heje, 2005:185-186), which has borrowed theories from reference disciplines such as computer systems engineering, computer science, social science disciplines such as sociology, anthropology, and psychology - instead of developing IS-centric theory from within the discipline (Avison & Pries-Heje, 2005:190-192). This makes the IS discipline both emerging in many of its aspects and also a pluralist discipline. Hence, the terminology of its concepts can be misinterpreted given different views on their original disciplinary meaning.

The concepts such as information systems (IS), information and communication technologies (ICT), information security, competencies and security e-competencies,

users and end users, and higher education institution (HEI) will be discussed in the following sections to explain their meanings in relation to this research:

1.2.1 Information Technology (IT), Information Systems (IS), and Information and Communication Technology (ICT)

By original definition, the term Information Technology (IT) refers to the technological side of an information system (Turban & Volonino, 2012:8) referring to the collection of computing systems that an organisation use. In the broadest sense, IT describes an organisation's collection of information resources, their users, and the management that oversees it all. Nemati (2008) refers to IT as all forms of technology (infrastructure) used to create, store, exchange, and use information in its various forms (business data, voice conversations, images, motion pictures, and other forms).

Concepts of communication resources also need to be added to the collective of IT resources because network and telecommunication resources are used to transfer information (Nemati, 2008). Thus it is also considered to be part of the IT resources. This research refers to IS and IT as Information and Communication Technology (ICT) (Jones, 2009) and applies the two terms interchangeably (IT, ICT) to refer to resources that are used in the HEI environment to process and transmit information. As ICT includes the IT resources, applications, network, and the internet to process and disseminate information (CEN, 2014c), IS is used to include the manual system of processing information to ICT resources.

For the purpose of this research, the IS concept is consistently used to refer to both automated and non-automated systems applied to process information in the HEI to collect, process, and distribute information (Doherty et *al*., 2009). In other instances, either IT or ICT is used to keep the original meaning of the ideas expressed by quoted authors or refer only to the technological systems. The term IS was selected as appropriate because end users need to be competent not only in one aspect of IS security, but in various aspects, both the technological and non-technological.

1.2.2 Information Systems security

The primary meaning of security refers to "*the quality and state of being secure and free from danger*" (Kabay & Whyne, 2009; Whitman & Mattord, 2010:3). It is also referred to as the state of being free from danger and not exposed to damage from accident or attack (Bosworth et *al*., 2009). On-going business processes require care and diligence in order to safeguard information and related systems from destruction, disclosure, and disruption (CEN, 2014c).

In the field of Information Systems, security refers to the protection of information and the resources in order to maintain their critical characteristics (confidentiality, integrity, and availability) during the storage, processing, and transmission through to the application of security controls (Whitman & Mattord, 2010:4). This covers the protection of information, communication networks, and business operations against unauthorised access, misappropriation, modification, loss, and unintentional disclosure to assure its confidentiality, integrity, availability (CIA) (Humphreys, 2008, Turban & Volonino, 2012:123; Kouns & Minoli, 2010:13; Shelly & Rosenblatt, 2010:138).

Hence, in respect of the definitions discussed by other authors, this study has adopted the definition of IS security as follows: IS security refers to the application of technological and non-technological security measures to preserve the integrity, confidentiality, availability, authorised access, and misuse of IS resources in supporting the operations and performance of HEIs.

These definitions recognise the importance of security technologies, administrative procedures, and individual end users skills and behaviour in the protection of IS resources. This implies that the information systems security is a multidisciplinary field (Gollmann, 2011:39; Piccoli, 2012:28) in which the achievement of the desired security state is possible, or can only be studied, through the combination of different measures.

1.2.3 Competencies and IS security e-competencies

In general, competencies refer to a system of complex actions including the knowledge, abilities, and attitudes required for a successful completion of tasks (Chang et *al*., 2012). The concept of security e-competency can be derived from the combination of security and e-competencies which are defined as a combination of skills, knowledge and attitudes (Romani, 2009). Accordingly, in this research, ICT security e-competencies refer to the application of security competencies (knowledge, skills, and abilities) by end users to protect IS resources in its environment (both online and offline). Chapter Four describes these competencies in more detail.

1.2.4 IS resources end users

In some instances, the end user can also be referred to as *user* (Albrechtsen, 2007). End users are people who have legitimate access to an organisation's IS resources. They are also "*individuals or organisations that directly interact with a computer based information system as information producers or consumers*" (Yoon, 2009). They are considered as insiders, employees, or contractors (Ciampa, 2014:21; Sarkar, 2010) of the organisation with varying roles and access rights to perform direct or indirect activities on the IS resources (Williams, 2008; Avison & Pries-Heje, 2005:192).

In this research, end users are perceived as the outer layer of the broader security that is being applied to both proactively and reactively protect the IS resources in the HE environment. These end users' actions can have a critical effect on the IS resources. Hence, their level of IS security is critical in order to protect the IS resources that they access.

1.2.5 Higher education institution (HEI)

The Higher Education Institution (HEI) in this study refers to an academic institution as per definition of the South African Higher Education and Training Laws Amendment Act 23 of 2012 (Higher Education Act 101 of 1997) "as an institution that can awards qualifications that meet the requirements of the Higher Education Qualification Framework (HEQF) in South Africa". This is independent of the mode of

teaching and learning employed by the institution, as it can be full-time, part-time, distance, or the combination of these modes. The selected institutions for this study are the main four HEIs located in the Western Cape Province, namely HEI01, HEI02, HEI03, and HEI04 that are named through the codes to protect their individual identities.

1.3 BACKGROUND AND RESEARCH PROBLEM STATEMENT

Threats facing information and Information and Communication Technology (ICT) systems originate from various sources and at different magnitudes to affect the integrity of these important resources. Some of the sources of threats are the result of:

- Human errors and negligence (Wood, 1995) such as carelessness with password and IS resources (Rainer & Cegielski, 2013:85-86); and
- Intentional acts of people to perpetrate with the intention of stealing information and other resources, or cause damage for different reasons using security threats like viruses attacks, denial of services attacks, social engineers and phishing (Rainer & Cegielski, 2013:85-86).

Both human errors and intentional acts can be the result of rightful end users perpetrating specific actions. These perpetrations can have a tremendous effect on an organisation (Rainer & Cegielski, 2013:85-94; Beisse, 2010:16-20). Holtsnider & Jaffe (2007:358-359) share the following perspectives:

- Human errors or mistakes of employees pose a huge problem as the result of laziness, carelessness, or a lack of awareness concerning information security;
- With the existence of hundreds of potential threats to IS resources, IS security has become the responsibility of everyone in an organisation (Sedinić et *al*., 2014; Whitman & Mattord, 2010:2; Humphreys, 2008; Holtsnider & Jaffe, 2007:358). This creates a necessity for ubiquitous ICT security competent users. It creates a necessity for the supply of IS security e-competencies to the employees in HEI environment so that they can play an active role in the protection of the organisational IS resources. Furthermore it is the responsibility of HEIs to ensure that this inclusive approach to IS security is

integrated in their operations, starting from the hiring of new employees through to retirement or resignation; and

- The single and most valuable ICT security control is an effective and on-going end user education and training tool as it makes every member of the organisation aware of the vital importance of information (IS) security.

A failure to integrate end users in the protection of organisational IS resources, can create a trust deficit between the management of ICT resources and users which leads towards caused general ignorance of this important practices in many organisations. This can be due to the ICT security managers' beliefs that end users lack skills, motivation, and knowledge to practice secure behaviour when handling IS resources (Rastogi & von Solms, 2012). Hence, ICT managers formulate security policies and controls (e.g. detective, corrective, preventive measures) based on technological consideration (Ciampa, 2014:88). They consider the security technologies as the only defence mechanism for IS resources and ignore the needs for developing IS security e-competencies amongst end users (Rastogi & von Solms, 2012).

A survey conducted by Deloitte in 2007 on global ICT security, Padayachee (2012) revealed that the concern for ICT resources security has shifted recently from technological predominance to human elements. As 91% of respondents were concerned about employees' security weaknesses, and 79% of respondents cited human factors as the root cause of ICT security failures. Dhillon (2007:156) confirms that 47% of security breaches are caused by human error, mainly by employees (Colwill, 2009).

Given the knowledge gained by end users through the access of the IS resources (and also their knowledge of the organisation and its internal processes) they can bypass or change settings on the systems. This makes end users become more dangerous than external threats (Willison & Siponen, 2009). It is therefore logical to reason that if the security of organisational information resources is everybody's responsibility, then the isolation of end users presents a security threat to these resources.

The preliminary review of training and development calendars of two of the four HEIs that were investigated in this research from 2012 to 2014, showed no evidence of ICT security training for employees either before or during their employment. This negligence sets at stake thousands of valuable stakeholders' information (staff, students, and finance) as well as the ICT infrastructure which is applied to process the information.

At one of the four HEIs that participated in this research, an incident occurred in November 2013 in which an e-mail was sent informing the personnel that their salary package for the year is shown in an attachment. However, the attached zipped file contained executable malware. Unfortunately, administrative assistants in at least two departments opened the attached file before the computer services department has sent a warning e-mail. As a result, the two departments' computers were affected and became slow and could not print to the network printer and local network until technicians could resolve the problem the following day.

Another incident witnessed as researcher, involved an office administrator leaving her desk for more than twenty minutes with her login details (username and password) displayed on the screen. This could enable anyone to access a highly important organisational-wide integrated system with a click of the OK button.

In addition to the above cases as well as the references to other security breaches reported in Farn et *al*. (2008) and Harwood (2011:117), end users can be vulnerable if they are not educated, trained, and made aware of company policies and best practices. For this reason, many companies offer employees security training to help mitigate breaches. In fact, although IS security awareness (and training) is viewed as one of the most important information security management considerations, still less investment is often made towards end user training programmes compared to security technologies (Tsohou et *al*., 2012).

The mentioned threats to ICT resources in the HE environment such as carelessness with IS resources, theft of ICT and supportive resources (Ciampa, 2014), has prompted investigation into the current ICT security and e-competencies

development practices within the four selected HEIs in the Western Cape. Also, during 2012 to 2014 a preliminary pilot study at two of the four selected HEIs in the Western Cape revealed that no evidence of formal IS security e-competencies development exist at these institutions.

Apart from the perceived lack of ICT security e-competencies among the end users in the HEI and lack of plan to provide such needed security e-competencies, the second problem addressed in this research relates to the absence of theories, frameworks or models to guide the addressing of the identified end user related IS security issues. Hence, this study undertook the development of an ICT security e-competencies framework that can comprehensively address the IS related organisational security issues in the HEI environment.

It is important to state that, presently there are a number of frameworks that , in a limited manner, address the security e-competencies of ICT professionals such as Skills Framework for Information Age (SFIA) and the European e-Competencies Framework (e-CF). However, the ICT security e-competency framework for end users and their development in the HEI environment is yet to receive deserving research attention as an important component of IS security programme.

It is therefore reasonable to presume that the HEIs that rely on these IS resources and the Internet, are exposed to and affected by various security threats and security breaches that could have been prevented or addressed through IS security e-competencies. The current HEIs ICT security practice based on the reliance on security policies (Xiao-yan et *al*., 2011; Herath & Rao, 2009) or security technologies protection (Okenyi *et al*., 2013; Coles-Kemp, 2009; Rhee *et al*., 2009) have been proven problematical and only involve human related factors to a minimum if at all. The ICT security related errors and weaknesses (Smith, 2009) such as writing down and sharing password or employees carelessness with mobile IS resources such as laptop (Rhee *et al*., 2009) cannot be successfully addressed without including e-competent end users.

This recognition acknowledges the importance of finding ways to improve the security of IS resources in the HEI environment that moves beyond the mere focus on security technologies. This study identifies the IS security e-competencies at appropriate levels of work that employees (end users) perform in various departments of the four selected HEIs. The study also designs suitable training methods that can reach the maximum number of end users in the HEI environment.

This research investigates the ICT security e-competencies development practices of the four HEIs in the Western Cape with the intention to develop an IS security e-competencies development framework that is capable of addressing the ICT security needs of end users in the HEI environment.

1.4 AIM AND OBJECTIVES OF THE STUDY

While a number of researches on ICT security "*focus on either technological, algorithm and building secure infrastructures or security threats*" (IJHCS, 2007; Rehman et *al.*, 2014; Theoharidou, et *al*., 2014), this research aims to explore the end users' IS security e-competencies necessary to safely operate in the digital environment and create a conceptual framework for security e-competencies for Higher Education Institutions (HEIs). Accordingly, these security e-competencies and the ways they can be supplied to end users in the HE environment need to be identified and incorporated into the final framework to be proposed.

1.4.1 Research objectives

In response to the problem statement and aim mentioned in previous section, this research aims to achieve the following objectives:

- To explore the IS security e-competencies development practices of the four Higher Education Institutions (HEIs) in the Western Cape.; and
- To develop a conceptual framework which not only identifies IS security e-competencies, but also demonstrates how it can effectively be supplied to the end users.

The development of such an IS security e-competency framework is considered as a key factor for the development of e-competencies required to protect IS resources. It

is also regarded in this research as a key factor for human capital (HC) improvement (Saldaña-Ramos et *al*., 2014).

1.4.2 Research sub-objectives

In order for this research to achieve its main objectives, the following sub-objectives were set:

Sub-objective 1: To analyse the importance of IS resources and their security in the HEI environment, which include:

- The analysis of the importance of IS resources in the operations of the HEIs;
- Determining which ICT systems in the HEI environment are critical and have been classified as such; and
- Determining, from the IS security experts and end users individual responsibilities necessary to protect the IS resources.

Sub-objective 2: To investigate the IS security e-competencies' development of "best practices" in general and how they are currently implemented by the participating HEIs. This includes determining:

- Whether the end users have been formally trained in IS security at their respective Higher Education Institutions (HEIs);
- Whether end users have been trained in ICT security policy;
- The challenges that HEIs face that affect the development of IS security e-competencies;
- The major threats affecting the information resources (ICT resources) at the HEI and how they are dealt with; and
- How the IS security experts rate the institutions' commitment to the development of IS security e-competencies.

Sub-objective 3: To develop optimal ways of supplying IS security e-competencies in the HE environment, including determining:

- Who the key end users of IS resources are, and how they can be classified according to their responsibilities and needs for IS security e-competencies;

- The importance of IS security e-competencies development for the end users and the institution;
- The challenges experienced when staff members are trained;
- The content of IS security e-competencies development from the IS security experts point of view;
- The current practices and approaches that the training and development department and institution have adopted to provide training to employees; and
- The methods that are being applied to provide training to employees in the HEI environment and how effective these methods prove to be in meeting the current needs and those of IS security e-competencies development.

1.5 RESEARCH QUESTION AND SUB-QUESTIONS

In order to achieve the research objective and sub-objectives derived from the problem statement, the following main research question has to be addressed:

What Information Systems security e-competencies are needed in Higher Education Institutions (HEIs) for effective protection of IS resources and how can these security e-competencies be supplied to end users?

1.5.1 Research sub-questions

The research sub-questions are categorised into three categories which are linked to the research sub-objectives. Each of the sub-questions is linked to the main research question. The sub-questions and their three main categories are:

Sub-question 1: What is the importance of IS resources and their security in the HEI environment? In order to answer this sub-question, the following questions were asked:

1.1. What is the importance of ICT resources in the operations of the HEIs?
1.2. Which ICT systems are critical and have been classified as supportive to the operations of HEI?
1.3. Whose responsibility is it to protect the IS resources in the HEI?

Sub-question 2: What are the IS security e-competencies development practices in the participating HEIs. In order to answer this sub-question, the following questions were asked:

2.1. What are the major threats that affect the information IS resources of the participating institutions?
2.2. How do the participating institutions address ICT security threats that affect their IS resources?
2.3. Was formal IS security training provided to the IS resources end users in the participating institutions?
2.4. What training has been provided to the end users regarding security competences?
2.5. What challenges did the participating institutions experienced during the development of IS security e-competencies?
2.6. What is the institutions' commitment to the development of IS security e-competencies?

Sub-question 3: What are optimal ways of supplying the required IS security e-competencies in the HE environment. In order to answer this sub-question, the following questions were asked:

3.1. Who are the key end users of IS resources and how can they be classified in terms of their responsibilities and needs for IS security e-competencies?
3.2. What is the importance of IS security e-competencies development for the end users?
3.3. What is the importance of IS security e-competencies development for the institution?
3.4. What are the challenges experienced when training end users?
3.5. What is the content of the IS security e-competences training?
3.6. What are the current practices and approaches towards competency development that the training and development department and the institutions have adopted?
3.7. How effective is the applied training method in developing IS security e-competencies?

1.6 OVERVIEW OF RESEARCH DESIGN AND METHODOLOGY

The research design sets a plan for the research execution, data collection, and analysis to help achieve the research objectives (Jankowicz, 2005:196; Blanche *et al.*, 2006:34; Flick, 2011:50, 68-69). This section gives a brief description on the research methodology and strategy, data sources, and data gathering techniques and will be extensively explained in Chapter 5.

The design of this study included the following:

- In the initial phase, the existence of and need for IS security e-competences was explored at two of the four participating HEIs in the Western Cape.
- Next, the research problem was identified and research objectives and questions were established.
- An initial literature review was done in order obtain a sense of possible research methodology and the need for a theoretical approach.
- An extensive literature review was conducted in order to theoretically answer the established research questions. This was done in accordance to the selected theoretical lenses, namely the Activity Theory.
- This was followed by the selection of the research methodology and construction of the data gathering instruments.
- Thereafter, the collected data was analysed, followed by reporting on the findings, conclusion and recommendation.

1.6.1 Research method and strategy

A research project can be approached from a qualitative or quantitative methodological perspective. The difference in either methodology is how the researcher reports on what occurred (participants' involvement) or analyses what has occurred (interviews or narrative of the participants) (Miller & Brewer, 2003:192; Flick, 2011: 92) and reviews previous documents on the research topic as a secondary data collection technique.

This study's methodology was determined by the nature of the research problem. Hence it was anticipated that neither quantitative nor a qualitative methodology on their own would successfully answer the research questions and meet the research

objectives. Therefore, this study applied a mixed methodology (Somekh & lewin, 2006:274).

A mixed method research approach, which is also referred to as a triangulation approach is supported by authors such as Myers (1997), Cooper & Schindler (2006:219) and Venkatesh et *al*. (2013:21-54) because it helps to develop a rich insight into phenomena of interest that cannot be understood using a single method. The intention was to overcome the weaknesses of each approach and increase the validity of research results (Willis, 2007:219). The mixed method approach was executed through the application of the multiple case study methodology (Henn et *al*., 2006:58).

The mixed research approach is appropriate for this research (IS security e-competencies development) which by its nature is sensitive and has the objective of reaching a broad participation as well as gaining an in-depth knowledge from experts from different HEIs. In this regard, there was a constant comparison of the answers collected from in-depth interviews and survey to establish how they help in confirming the current practices and establish with accuracy the way of improving and answering research questions.

In accordance with the selected methodology, the data were gathered by interviewing the key informants including the IS security experts, the training and development practitioners, the university council representative (registrar), and the legal services of each of the four HEIs. This category of participants was interviewed using an in-depth interview technique which lasted about one hour. The quantitative data were gathered through a research survey that was administered to the IS resources end users who were identified during the interviews with the IS security experts from each HEI.

The data were analysed by using the Content Analysis (CA) and Grounded Theory methods of the pattern identification (categorising), and constant comparison, coding.

1.6.2 Overview of the underlying theory

To understand and interpret the various constructs that interplay to achieve success with the supply of IS security e-competencies in HEI context; this research applied the Activity Theory (AT) as its underlying theory. The AT as presented in Figure 1.1, with the addition of basic questions, helped in discovering the critical factors and their influence in achieving the objectives of this research. This study adopted AT because it is "*an integrated conceptual and methodological framework for understanding the complex interactions*" between various constructs and the sustainability of knowledge creation practices (Timmis, 2014). In this research, the constructs include people, policies and other documents, as well as the tools that are applied and that interact with development ICT security e-competencies needed by either the end users or the object of IS security e-competencies development activity. In this regard, the AT was used as a tool to study the role of the agency in achieving the object of the activity (Shankar et *al*., 2011).

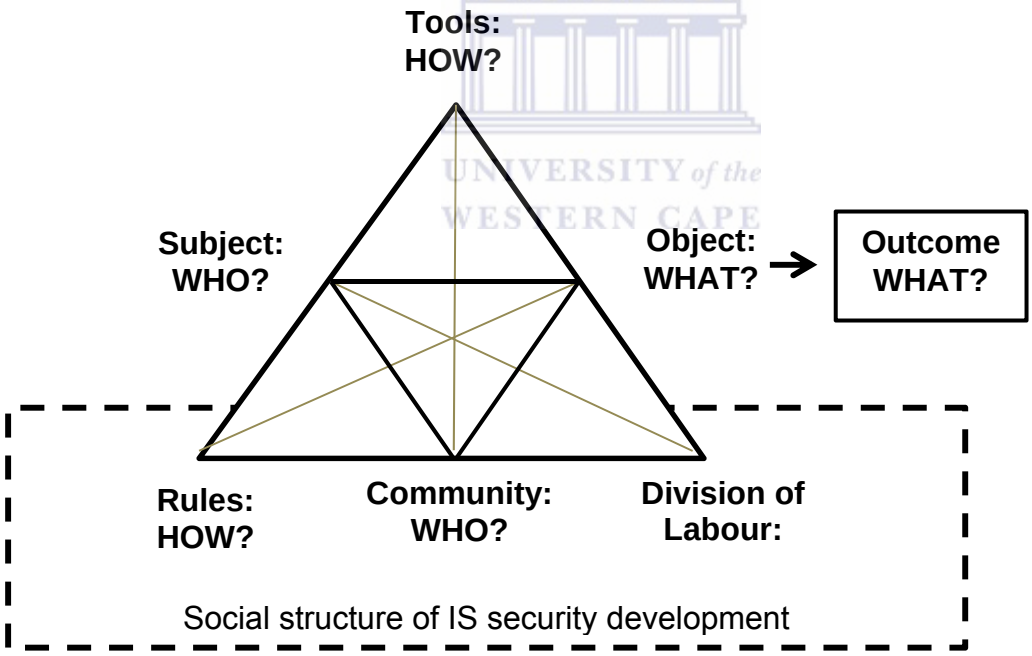


Figure 1.1: Theoretical framework based on the activity system

(**Source**: Adapted from Sun & Qu, 2014 and Paraskeva et *al*., 2010)

The AT was applied in this research at its collective level as opposed to its individual level (Peña-Ayala et *al.*, 2014) that presents the individual system as made up of the grouping of four elements: subject, tool, object, and outcome. At a collective level,

the AT framework becomes a systemic model of an activity system (Peña-Ayala et *al*., 2014). In this instance, agents in the activity theory interact with each other to create a community with the intention to achieve a common object through the intermediation of tools, respect of rules and division of labour (Sun & Qu, 2014).

The subject in Figure 1 represents an individual responsible for the activity; the object unveils the objective and motive for the activity; tool represents an artefact facilitating the achievement of the object, and the outcome represents the result of the transformation process. To these three initial elements of the theory, the layer made of three elements (rules, community, and division of labour) of the system was added to regulate the interaction between the constructs of the system (Sun & Qu, 2014; Park et *al*., 2013).

Peña-Ayala et *al*. (2014) explained the role of the three additional elements and points out that the rules-element guides the actions of the subjects to achieve the object. The community represents those that engage in the activity while the division of labour assigns the roles to members of the community.

Activity Theory assisted in the creation of a conceptual framework that can be applied to assess the reason(s) for the participating HEIs' successful or unsuccessful achievement of IS security e-competencies development objectives. Consequently, this research believes that Activity Theory (AT) is an appropriate model for studying ICT e-competency and their interconnection with other components of the HEI.

1.6.3 Research assumptions

One of the agreements that qualitative and quantitative researchers have reached according to Johnson & Onwuegbuzie (2004) is the Duhem-Quine thesis or idea of auxiliary assumptions. In this research study, the mixed research method is applied to predict the future or, in other words the assumptions are used to guide the set objectives in reaching a research conclusion. For that reason, the pre-set assumptions associated with this study, are:

- ICT security e-competencies are just as important for HEIs as they are in any other institutions that rely on IS resources to conduct their business.

Therefore, HEIs need to include the end users of IS resources in the security programme of IS resources, and continuously keep them in the supplied with relevant IS security e-competencies to ensure their relevance in the changing ICT environment.

- The existing focus of IS resources security at the HEIs is predominantly based on technology security measures.
- The HEIs do not have a formal model for the development of security e-competencies and the integration of these security practices into their IS security operations.
- The development of end users' security e-competencies for the protection of IS resources in the higher education context can create a permanent awareness of the importance of information security with reference to higher education environment and challenges.
- IS security e-competencies are better supplied when they are identified in a framework that models the skills for the category of end users as it exists in the HEI environment.

1.6.3 Ethical considerations

Throughout this research, the researcher recognised interaction at different levels between participants. Different organisation's shared the valuable information they own and control with each other. Therefore, it was essential that the participants (HEIs, individuals, and their information) were protected from any form of abuse, harm, misrepresentation and unintended usage apart from the achievement of this research's objectives and the production of knowledge as explained to participants in the consent form before each interview and questionnaire.

At all times, in striving to achieve the research objectives, this research remained within the University of the Western Cape's (UWC) ethical guidelines whenever interacting with participants, accessing stored and published information, or throughout the codification, analysis, and allocation of meanings and the collected information as they relate to IS security e-competencies.

The social science research principles for ethical study of Someth & Lewin (2006:3, 56-57), Flick (2011: 214-227), and Saldana (2009:29, 38) were followed throughout this research and are stipulated below:

- Informed consent from the participants: voluntary participation from each participant was obtained by explaining to each participant in advance the purpose of the research and the extent to which the information was to be used. A consent form was signed by each participant before the interview and completion of questionnaire to confirm their voluntary participation.

- All information was treated as confidential and anonymously. The names of participants and their respective institutions are not mentioned or revealed. Wherein views and contents from other researchers were used, these sources were authentically acknowledged with references.

As part of following good ethical principles, this research received the ethical clearance from the research committees of each of the four participating HEIs before data colleting. With reference to this research's ethical compliance, the Senate Research Committee of the UWC issued an ethic clearance certificate (see Appendix A).

1.7 BRIEF FINDINGS FROM THE STUDY

The following sections discuss the literature review as basis for the research with the empirical viewpoints to follow.

1.7.1 Brief findings from the literature

There exists a great deal of relevant information which was collected through the review of the pertinent literature. This is presented in the first three chapters of this thesis. The key findings from the literature review are:

- The effective security of Information Systems (IS) resources in any organisation is a result of the appropriate combination of both technological security controls and human (i.e. IS resources end users) competencies.
- There was no single framework found in the relevant literature that could be used in the HEI context to assess or develop the IS security e-competencies

of the end users. The skills frameworks related to the IT industry, such as Skills Framework for Information Age (SFIA), general IS competency frameworks, the European e-Competence Framework (e-CF), or the International Council on Systems Engineering (INCOSE) frameworks are either too broad or too focused on the security e-competencies that IT professionals need to the exclusion of the needs of end users.

- The IS security e-competencies development framework proposed in this study followed the recommendations for effective framework development of Holt & Perry (2011:103-121), which suggested the following prerequisites:
    - **A purpose**: which in this research is to develop the IS security e-competencies of the IS resources end users.
    - **Identified the stakeholders and their profile**: which in this research are the HEIs employees in the end user institutional department.
    - **Identification of the sources framework**: this research used the general frameworks such SFIA, e-CF, and INCOSE its source frameworks.
    - **Identification of relevant competencies**: in this research the relevant competencies were identified and classified in four spheres, which include: (i) technology sphere, (ii) security policies and procedures sphere, (iii) environmental sphere, and (iv) cultural sphere.
    - Finally, the setting of competency levels: the proposed framework (Figure 7.2) identified three levels of IS security e-competencies for end users: **Level 1** which includes the general administrative staff members and academic staff who access information to perform their duties; **Level 2** which includes the information managers or officers; and **Level 3** which includes the departmental heads (called information curators) who set the roles, access right, and operating procedures for information in their departments.

- The findings from the literature reviewed for this study also suggest that the IS security e-competencies of end users is a result of the combination of (i) knowledge, (ii) skills, and (iii) attitude and behaviour (Chang et *al*., 2012; Holt & Parry, 2011:1; Sabeil et *al*., 2011). This makes the end users capable of

protecting the IS resources that are accessed in the organisational environment. It is mportant to consider that these three components do not operate in isolation. The knowledge element of a competency, which is the theoretical understanding and awareness of IS resources threats and security measures applied to protect the IS resources, can be used by the end users to develop skills, which demonstrate their ability to apply what they know (Ala-Mutka, 2011). The literature reviewed in this study also suggests that 'attitude' and 'behaviour' should be embedded in knowledge and skills.

Finally, literature reviewed showed that the best way to supply IS security e-competencies is through combined methods of delivery to accommodate different learning styles and to reach isolated employees across various campuses and sites.

1.7.2 Brief findings from the empirical study

The findings from the empirical study can be summarised as:

- The representatives from the four HEIs examined suggested that IS resources are important and are core to the operations of HEIs. These HEIs' administration, teaching and learning, and research are all based on the proper functioning and secured IS resources. In addition the ICT security experts acknowledged that the end users are an important part of the security of IS resources in the HEI environment.
- In contradiction to the findings from the literature reviewed, the HEIs examined here have not formally supplied IS security e-competencies to the end users, but have relied on the security technologies to protect their IS resources. According to the literature reviewed, this is not an effective way for obtaining IS security as the security technologies alone are not effective in deterring internal end users' mistakes and their inability to handle related IS resources.

Given that the end users are important in the process of protecting the organisational IS resources of the HEIs, this research applied the findings from the literature and empirical study to suggest an IS security e-competencies development framework (Figure 7.2). The framework specifically identifies security e-competencies required

and the way in which they could be supplied to end users within the particular context and challenges of the HEI environment. In this manner, the study has answered the main research question: “What Information Systems security e-competencies are needed in Higher Education Institutions (HEIs) for effective protection of IS resources and how can these security e-competencies be supplied to end users?”

1.8 CONTRIBUTION OF THIS STUDY

This research contributed to the body of knowledge of information systems as it provided a IS security competences framework which includes the identification of these competences as well as the proposition of the method of appropriately developing and supplying IS security e-competences to the end users.

Theoretically, this study has raised the importance of developing IS security e-competencies in the HEI setting, and it has provided a foundation framework for formal integration of IS resources end users into the IS security programme of HEIs as a practical implementation pathway. To date this practical aspect has been neglected while the end users are recognised as important role players in the security of IS resources. Furthermore, this research supports the idea of continuous development of IS security e-competencies among the end users to strengthen their degree of resistance to the dynamic world of security threats that HEIs face in their reliance on IS resources for general administration, teaching and learning.

1.9 RESEARCH DELIMITATION

The field of information systems (IS) and information systems security has developed faster than any other field in the last decade due to the various challenges and needs of organisations operating in this modern networked economy age. Hence, much has been written and published in the IS field and many sub-fields have emerged from this specific field. This research could not explore all the full gamut of all of these areas and has focussed its effort on an important and definable topic.

It was essential for this research to focus on its aim and objectives to avoid any unnecessary broadening of the scope of study. Therefore, this research focused on the exploration of IS security e-competencies development practices of the four HEIs in the Western Cape with the aim of developing an IS security e-competencies development framework for IS resources for end users. The study's target audience inevitably limited the generalisation of results to the Western Cape Province though the results may be applicable to other HEIs in South Africa.

Due to the large population encompassing end users at the four HEIs, the sample method had to be purposely limited due to the:

1. Feasibility as it would be a complex and unfeasible task to contact everyone in the targeted populations;
2. The policy-related time constraints in the academic institution and time required when dealing with a larger number of a sample;
3. Quality in relation to the number of participants and data collection. The higher the volume of data that are collected the more challenging it becomes to consolidate and make a reliable decision; and
4. Costs involved in traveling, contacting, and following up with the participants from various provinces could be high.

However, it is considered that these limitations have not influenced the validity of the study and posits that the findings are empirically relevant.

1.10 THESIS OUTLINE

This research thesis has been structured in the following way:

1. CHAPTER ONE – INTRODUCTION AND BACKGROUND: This chapter provides a general perspective about the topic, objectives of the study, the research problem, research questions and sub-questions which are answered. A brief description on findings from both literature and empirical studies from this research are also presented.

2. CHAPTER TWO – UNDERLYING RESEARCH THEORY: In this chapter the usefulness of social science research theories in analysing the research

problems is addressed. The chapter focuses on Activity Theory (AT) and how it contributes to the identification of the interplay between the various components of IS security e-competencies development activities and how the components contribute in the achieving of IS security e-competencies development object.

3. CHAPTER THREE – LITERATURE REVIEW: SECURING INFORMATION AND COMMUNICATION RESOURCES IN THE HIGHER EDUCATION CONTEXT: This chapter presents a general overview of the different approaches to the security of information systems (IS) resources in general. It also focuses on policies, security technologies, and the impact of human behaviour in securing the IS resources. These aspects of security are discussed in order to identify the IS security e-competencies to be supplied to IS resources end users and answered the research sub-questions 1 and 3.

4. CHAPTER FOUR – LITERATURE REVIEW: COMPETENCY FRAMEWORKS AND THE SUPPLY OF SECURITY E-COMPETENCIES IN HIGHER EDUCATION ENVIRONMENT: Chapter Four investigates the different competency frameworks with the intention of identifying one that addresses the IS security e-competencies for the organisational end users. It focuses on the discovery of the structures to be included in the final framework for IS security e-competencies development in the HEI environment. Furthermore, the chapter presents the methods appropriate for the supply of a IS security e-competencies developmental programme that can reach a maximum number of end users in the HEI environment. These end users are dispersed across various campuses and prefer different learning styles. In discussing these topics, the chapter answered the research sub-question 3 on the levels of competencies.

5. CHAPTER FIVE – RESEARCH DESIGN AND METHODOLOGY: This chapter describes the research methods that were applied in the empirical phase of this research. The chapter explains the selected research approach and its importance for the IS security e-competencies development. Also, the

techniques for data collection and analysis are set out in accordance to the combined research method within the multiple case study methodology.

6. CHAPTER SIX – DATA COLLECTION AND ANALYSIS: Chapter Six describes the empirical data that was collected, from the IS security experts from other HEIs, as well as the results from the in-depth interviews and survey questionnaires completed at the HEIs. The chapter also discusses the difference in quantitative and qualitative data analysis and the validity of each for this research.

7. CHAPTER SEVEN – FINDINGS AND INTERPRETATION: This chapter debates the findings and suggests the IS security e-competencies developmental framework that can be used in the HEI environment for the development of end users IS security e-competencies.

8. CHAPTER EIGHT – CONCLUSION AND RECOMMENDATIONS: In Chapter Eight a final conclusion is reached and recommendations are made. The chapter acknowledges the contribution and limitations of this research and also suggests the direction for future research in the area of the IS security e-competencies.

1.11 CHAPTER SUMMARY

This chapter has laid a foundation for the understanding of the research tittle, its aims, objectives and the basic terminologies that are used throughout the study. It also positioned the base for the research method that was applied and provided the outline of the content to follow.

In this chapter the importance of IS security e-competencies development as a fundamental aspect of IS security for any business organisation was proposed. This is important as the lack of IS security e-competencies from the internal end users is seen as a vulnerability in the protection of IS resources and a threat to the availability of the information and the resources that process them. Activity Theory (AT) was

presented in this chapter as the theoretical basis on which the IS security e-competencies framework components are built.

I established ethical considerations for this research that helped in guiding the researcher in the application of an appropriate standard of research ethics from the drafting of research questions, interaction with participants, administration of research questionnaires to data analysis and reporting.

CHAPTER TWO: UNDERLYING RESEARCH THEORY

2.1 INTRODUCTION

This chapter focuses on the description of Activity Theory (AT) which was applied as the research lenses for the analysis of the IS security e-competencies development practices in the HEI environment. In particular, the description focuses on the components, principles, and how AT was used to analyse and understand the interplay between the different stakeholders and other constructs that influence the development of IS security e-competencies in the HEI environment.

There are two reasons that led to the selection of the AT as an appropriate theory for this research: the first reason is its use of inductive reasoning and qualitative method (Hayden, 2014:4) which was selected as one of the mixed research methods in this study. The second reason is the social context in which the IS security e-competencies development takes place. This requires the use of socio-cultural (social) theory to understand the interplay between the constructs of the activity (Tsohou, 2012; Paraskeva et *al*., 2010; Paña-Ayala et *al*., 2014).

In relation to Activity Theory, this research advocates the overarching activity system (OAS) which combines two activity systems. These represent the way in which the main activity system and the other constructs interact and relate to each other in the development of IS security e-competencies among the employees in the HEI environment.

2.2 GENERAL PERSPECTIVE OF THEORIES IN RESEARCH

To understand the usefulness and the application of a theory and its appropriateness to this research, it is important to understand the difference between a theory and a model, which are often used interchangeably to provide a meaning to a concept (Hayden, 2014:3). West & Brown (2013:24) refer to the concept theory and model in this way: "*a model is a representation of a system, an object or characteristic set of events and it need not to explain anything*". On the other hand the authors say that "*a theory seeks to explain and predict (an event or a system) by proposing the existence or operation of entities that have not been observed*".

The understanding and application of theories (in the academic and professional discourse) is essential because they provide the foundation for professional practice. Theories help to develop approaches to solve problems and to formulate interventions to best provide the services (Hayden, 2014:1). Using Engerström (1987, 1993) as a reference, Paraskeva et *al*. (2010) states that "*AT appears to be a theoretical framework for understating how human activity is mediated by both tools and cultural context*".

Drawing from Hayden (2014:2-4), theory can be defined as "*a set of statements or principles devised to explain a group of facts or phenomena, especially one that has been accepted and can be used to make predictions about natural phenomena*". Glanz, Rimer, & Viswanath (2008:26) also provide a useful definition of theory as cited in Goodson (2010:5) and Acevedo (2012:242): "*A theory is a set of interrelated concepts, definitions, and propositions that present a systematic view of events or situations by specifying relations among variables in order to explain and predict events*".

Drawing from the use of theories as models for studying health promotion and disease prevention from Hayden's (2014:2) perspective, the theory in IS security e-competencies development can also be used to study the interplay between the artefacts in the HEIs' environment that contribute to the development of IS security e-competencies for end users. This can lead to behavioural (building their knowledge, skills, and behaviour – e-competencies) change and building the first line of defence against threats that IS resources face. This is of central importance to the delivery of teaching and learning, and administration services in the modern HE environment.

2.3 PERSPECTIVE ON ACTIVITY THEORY

This section focuses on a general description of the components of AT, fundamental principles, and also its application in the development of IS security e-competencies in the HEI environment.

2.3.1 Historical background of Activity Theory

AT has evolved from the psychological concept of the social nature of human subjects that are shaped by culture, influenced by language, acting with other people in organisations, groups, and communities (Allen et *al*., 2011). The first generation of AT was developed through the work of Russian psychologist researcher Vygostky around the years of the 1920s when explaining the idea of mediating artefacts (tools) had over the simple stimulus response model of behaviour (Stuart, 2004; Sun & Qu, 2014). AT was initially based on the role of tools and artefacts in mediating human actions and role of other people on mental activities (Timmis, 2014).

The first generation AT (Figure 2.1) was a triangular form and was based on the original model of the theory explaining how people use artefacts (tools) such as signs and shovels to mediate human action (Vygotsky, 1986 as cited in Ash, 2014). In Figure 2.1, the subject uses tools (mediation) to achieve the object. The first model was limited to the representation of the individual who was embedded in the activity (Stuart, 2004) then it was expanded to be used in the community environment where there is a unity of action (Sun & Qu, 2014).

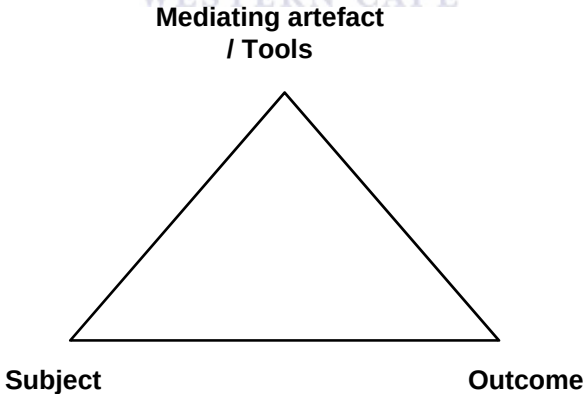


Figure 2.1: First generation of Activity Theory

(Source: Adapted from Johassen & Land, 2012:244; Nardi, 1996:26-28; Clark & Fournillier, 2012; Allen et *al*., 2011; Paraskeva er al., 2010)

The extension of the initial AT model was made possible through the work of Engeström in 1987 (Allen et *al*., 2011; Park et *al*., 2013) with the creation of the second generation of AT which added the layer of rules (norms), community, and

division of labour. This model still maintains the social context of activity and interaction between the subject and the other constructs in the context of the activity system with tools, rules, and division of labour inter-mediating the interactions between subjects and object, subjects and community, and between community and object respectively (Park et *al*., 2013).

The third generation of AT, which was selected for this research, "*focused on dialogue and the multiple perspectives of participants*" (Engeström, 2001 as cited by Sclater & Lally, 2013) in a composed activity system. It also "*describes how two related activity systems (interdepend) interact to solve a joint practice problem*" (Engeström, 2001 as cited in Reid, 2012). In the context of this research, there is one activity system that represents the end users who are intended to develop IS security e-competencies. On the other hand, there is an activity system representing the suppliers of the IS security e-competencies, represented by the HEIs. Both activity systems appear as interdependent, have different objects, but contribute to the same outcome.

With reference to the ideas of Allen et *al*. (2011) and Stuart (2014), AT is portrayed as a suitable framework for studying activity as it takes account of complexity, systemic approach, and development taking place in the system. Of importance, given the dynamic and fast changing ICT environment, AT is an appropriate theory for studying the development of IS security e-competencies, as there are innovations in the ICT and threats and the subsequent need for the protection measures. This is particularly important as the ICT field and the threats are dynamic and constantly changing, which requires a continual process of development of IS security e-competencies among the end users in the HEI environment.

2.3.2 Components of Activity Theory

From the perspective of theory in general, Hayden (2014:8-9) says that each theory has at least one concept at its core, and a series of constructs that indicate how the concepts are used in that theory. As an example to clarify the idea, the author uses the analogy of a house, namely, the theory is the house and the concepts then the

bricks. The way the bricks are assembled to build the house, will form the constructs.

Activity Theory (AT) follows this order of idea as it is made up of six components (Park et *al*., 2013; IRMA, 2012: 165; Whitton, 2014:145-146) which are: subject, object, tools, rules, community, and the distribution of labour. To these six components, the outcome has been added as the seventh component (Verdon, 2014). The model is presented in Chapter 1 (Figure 1.1). These components are briefly discussed below as the foundation and through the explanation of Shankar et *al*. (2011), Verdon (2014), Allen et *al*. (2011), Liaw et *al*. (2010):

- **Subject:** In AT, the subject represents a person or a group of people working toward the achievement of the activity's object (Hasan & Pfaff, 2012; Verdon et *al*., 2014). With reference to the second generation model, it is created by a community that is driven by a unity of purpose (Sun & Qu, 2014) and interacting together to achieve a common object. In this research, the subjects involved in the achievement of the object in the IS security e-competencies development activity include the end users (trainees), the training and development officials and the IS security experts who participate in the training and at the same time represent the institution.

- **Object:** According to Slater & Lally (2013), AT is a theory of object-driven activity. The object of AT is the meaning-giving purpose that distinguishes one activity from another and makes a motive for that activity (Timmis, 2014; Whitton, 2014:145). It refers to what the subjects do during the activity and represents the goals that the subjects pursue (Park et *al*., 2013).

  The referred object can be a material thing, but also less tangible item like a plan or intangible item like an idea. The importance is that it can be shared for manipulation and transformation process. In the words of Peña-Ayala et *al*. (2014), it unveils the activity's objective and motive for the transformation of an object into an outcome motivates the existence of an activity (Shankar et *al*., 2011).

In the case of this research, the objects are considered from the perspective of the activity systems that interact to achieve a common outcome. At one hand there are end users who need IS security e-competencies, and at the other hand there is the institution that, through its experts and training and development department supply the competencies. These two sides represent the two interacting activity systems working toward the achievement of the common outcome but with two different objects.

- **Tools:** This refers to the mediating artefacts in AT (Johassen & Land, 2012:244; Whitton, 2014:145-146) and can be anything that the subject(s) use in the object's transformation process. For instance, material tools and tools for thinking (Singh et *al*., 2009; Shankar et *al*., 2011). A tool can be "*physical, mental, semiotic, or speech and act; used to transform a situation*" (Siyahhan, 2010). They are used to mediate the subject's interaction with the object (Paraskeva et *al*., 2010) and facilitate the achievement of the activity's outcome by the subjects (Peña-Ayala et *al*., 2014).

  In this research, the tools that can be used in the transformation and facilitation of IS security e-competencies development include the training materials (documents) and equipment such as computers and related security applications, workshops, Intranet and Websites, and notice boards. To be effective, these tools need to be formalised in the process of IS security e-competencies development to be accessible for the subjects. These tools are developed and shared between the subjects throughout training and other awareness activities (Sedinić et *al*., 2014).

- **Outcome:** Every activity system is focused on achieving an outcome which is the actual motivation for the activity to take place (Engeström, 1987 as cited in Verdon et *al*., 2014). Otherwise, it is the result of the object transformation process (Peña-Ayala et *al*., 2014). The outcome forms a feedback to the subject for engaging in the activity and its result is not always satisfactory to the subject (Spais, 2010) as the unintended outcome is possible.

- **Rules:** In this instance, rules cover both explicit and implicit norms, conventions and social relations, explicit regulations, standards, and relationships among the community members, policies and procedures within a community; and guide the subjects in how they should work on the object (Shankar et *al*., 2011; Verdon et *al*., 2014; Liaw et *al*., 2010). In effect, the rules regulate the interaction of group members in the community (Sun & Qu, 2014).

  In the context of IS security e-competencies development, rules describe to the agents and other constructs, what is allowed and not allowed in the development of IS security e-competencies and regulate the training process. This is why contracts, norms, laws and government regulations, culture, and policies are relevant for this component and the entire activity.

  Yoon & Kim (2012) also affirm that the organisational norms (which are shaped by the security policy) are shared among the employees and regulate the employees behaviour (rules in the AT model) and end users attitude (tools in the AT model) and have a significant impact on end users behaviour on computer security.

- **Community:** This item refers to the individuals and subgroups, the social context which the subjects belong to and where they share common interest and involvement with the same object (Verdon et *al*., 2014; Liaw et *al*., 2010). The community mediate activity through the division of labour (Paraskeva et *al*., 2010).

  The community is represented by the stakeholders in HEI and are involved in rendering possible successful development of IS security e-competencies (object). The community involve ICT security experts, ICT managers, nontechnical general business managers (Whitman & Mattord, 2010:3), as well as the employees, the human resources department (human resources development unit), finance and infrastructure, and other stakeholders in the institution whom support proves to be essential. Working together, these

stakeholders ensure that IS security e-competencies among end users in the HEI are continuously developed.

- **Distribution of labour:** This aspect relates to the assignment of roles and responsibilities among the members of the community who are within the activity system. It can be the horizontal division of tasks or the vertical division of power with reference to social status, qualifications, and knowledge of the object (Park et *al*., 2013). It is a construct that regulate the work of agents in the pursuit of common goal (Sun & Qu, 2014).

The last three components of AT were included to adapt the framework for the large community that work together for the fulfilment of a common object. As such, rules, community, and division of labour are described as the social structure (Sun & Qu, 2014) in the IS security e-competencies development.

AT recognises as its unit of analysis the existence of an activity to help with research focus (Singh et *al*., 2009). The activity according to Shankar et *al*. (2011) is comprised of subject, object, actions, and operations. Previous research already applied AT in learning environments and has considered learning as an activity (Liaw et *al*., 2010). This research considers the IS security e-competencies development as its unit of analysis. In other words, at the centre of AT is the activity system approach in which people (stakeholders) work together in groups to achieve an objective that is of common interest (Sun & Qu, 2014).

The interaction between the constructs of activity within the system or between different systems create tensions and contradictions which enable the subjects to innovate and create knowledge due to the start of new conception of activity which is called "*cycles of expensive knowledge*" (Engestrom, 2001). Therefore, the following section discusses some principles applied to AT to avoid unnecessary confusion and tension between its constructs.

2.3.3 Principles of Activity Theory

In its attempt to provide a pattern for demonstrating and analysing the interaction between the constructs in the achievement of the system's object, AT uses a set of principles as its foundation. Among the principles, Peña-Ayala (2014) highlights the following:

- **Object-oriented:** This principle represents achievement of the object as the reason for the existence and undertaking of an activity.
- **Hierarchical structure:** This presents the structure to guide the interaction between the individuals and the world (AT constructs) through the following three levels (activity, actions, and operations) with understanding that the three elements may take the status of each other at any stage and are not static (Allen et *al*., 2011; Timmis, 2014):
    - **Activity**: is the actions performed and form a collective system. In this instance, the object drives this collective system and the object comprises of the subjects that. Thus, activities are distinguished from one another through their objects. In the case of developing IS security e-competencies there is a need to perform more than one activity. Activities such as planning for training, delivery, assessment and review, financing, and those identified in the training process. Activities are governed by motives and can be at individual or collective level (Allen et *al*., 2011).
    - **Actions**: refer to conscious deeds that are carried out through operations and are goal(s) driven which means that one action could be distinguished from another (Allen et *al*., 2011). The IS security e-competencies development is only achieved when the subjects in the two activity systems (Figure 2.2) perform a set of actions.

      The actions in the case of IS security e-competencies development may include the identification of potential threats to IS resources and possible security measures to protect the resources. On the basis of these actions, the possible IS security e-competencies could be identified and developed among the end users. It is important to know that t threats and security measures evolve, hence the performance of

these actions and the development of IS security e-competencies is set to be a continuous process.

- **Operations**: are routine tasks of which its activation depends on the conditions of the action. Ultimately, it is the conditions that govern operations (Allen et *al*., 2011) and differentiate the one from the other (Timmis, 2014).

  In the case of this research, if the activity is to develop IS security e-competencies among the end users, then the identification of the possible threats to IS resources can be an action which requires users to perform operations such as conducting environment assessment.

- **Mediation:** is accomplished by the tools that facilitate activity (tools) and are used to control human behaviour (rules) and even the allocation tasks to be carried out during the activity (division of labour).
- **Internalisation-externalisation:** is the representation of human mental and physical actions of individuals during and after the activity. Allen et *al*. (2011) view these two actions as the result of an activity outcome.
- **Anticipation:** in this regard refers to future events or the improvement on the practices and tools.
- **Development:** produces human interaction with reality by mediation.

2.3.4 Motivation for applying Activity Theory in IS security e-competencies development

In this research, AT is applied for IS security e-competencies development as a conceptual framework in the quest to understand that human activities and participation (including those in HEIs) are driven by needs and are directed to an object (Allen, 2010) . The use of AT proved to be advantageous given the complexity of the development of IS security e-competencies in a multifaceted environment such as HEI, where thousands of end users are employed and dispersed across different sites (campuses), working in different departments and functional areas.

E-competencies development itself uses different mechanisms and technologies (workshops, training materials, online media, rules, hardware and software tools and techniques, and even standards and regulations) and different agents (trainers and participants). As such, though a complex undertaking the application of the socially oriented descriptive tool, AT, enables the understanding of the interrelatedness of the various role players for achieving the object. AT not only gives the flexibility to interplay tasks into activities (and the role of the agencies) which makes it easy to interpret and manage (Shankar et *al*., 2011) the agencies and their interactions, but also to manage the intended object.

The demonstration of applying AT in this chapter is limited to the understanding of the practices of IS security, legal requirements, and employee training and development rules (training schedules) as confirmed through the literature review and observation of the practices in the HE environment. To these elements, the spheres for IS security development to end users such as policies, technologies, culture, and the environment (both internal and external) which need to be considered when developing IS security e-competencies (Tshinu et *al*., 2014) were also taken into consideration.

The application of AT in this research assumed that the IS security e-competencies development, the security of IS resources, and ICT industry are dynamic and changes can occur at any given time. IS security e-competencies development can be achieved by applying various activities such as the following identified in the literature: awareness campaign, training and workshops, distribution of ICT security policies, and security assessment per term or semester. These activities could change according to the situation and other factors in the HE environment and ICT industry (threats and security) to realign the constituents of the activity (Shankar et *al*., 2011). This changing conditions suit well with AT, which emphasises the change rather than the stability as it focuses on the dynamics of learning as opposed to learner as a participant in an established system (Berragan, 2013; Jones & Holt, 2008).

As already stated, the application of AT in this research is based on its third generation model, which the IS security e-competencies development presented as a collection of two activity systems that are interconnected and inter-dependent to achieve a common outcome (Figure 2.2). This way of applying the activity system follows the same direction of comprehensive learning study which took as its unit of analysis a constellation of two or more activity systems that share the same object (Berragan, 2013).

Berragan (2013) points to the influence of tensions and conflicts when two activity systems are used in different communities with a different concern. To the contrary, the proposed Overarching Activity System (OAS) presents no such tensions and conflicts except in the case of deficiencies. This is because the two activity systems are subjected to the same community and rules within the same HEI environment, and mainly also because they work toward the achievement of the same outcome as presented in the Figure 2.2.

Figure 2.2 presents the conceptualisation of IS security e-competencies as an activity made of various artefacts working together to develop IS security e-competent end users. The theory conceptualises IS security e-competencies development as the overarching activity system (OAS) and consist of groups that cooperate towards a common outcome as (Saldaña-Ramos et *al*., 2014).

IS security training as intermediary tools (Tshinu et *al*., 2014), confirms the need for IS security e-competencies to be developed for the end user of IS resources to ensure the effective participation in protecting the IS resources.

Figure 2.2 presents a framework for understanding the interaction of the constructs relating to the successful development of IS security e-competencies among the end users in the HEI based on AT. The two interacting activity systems of the one overarching system engage the core activity by representing the two subjects that participate in the activity (end users and suppliers of IS security e-competencies – instructors and security experts), without whom the transformation of the object of the activity is impossible.

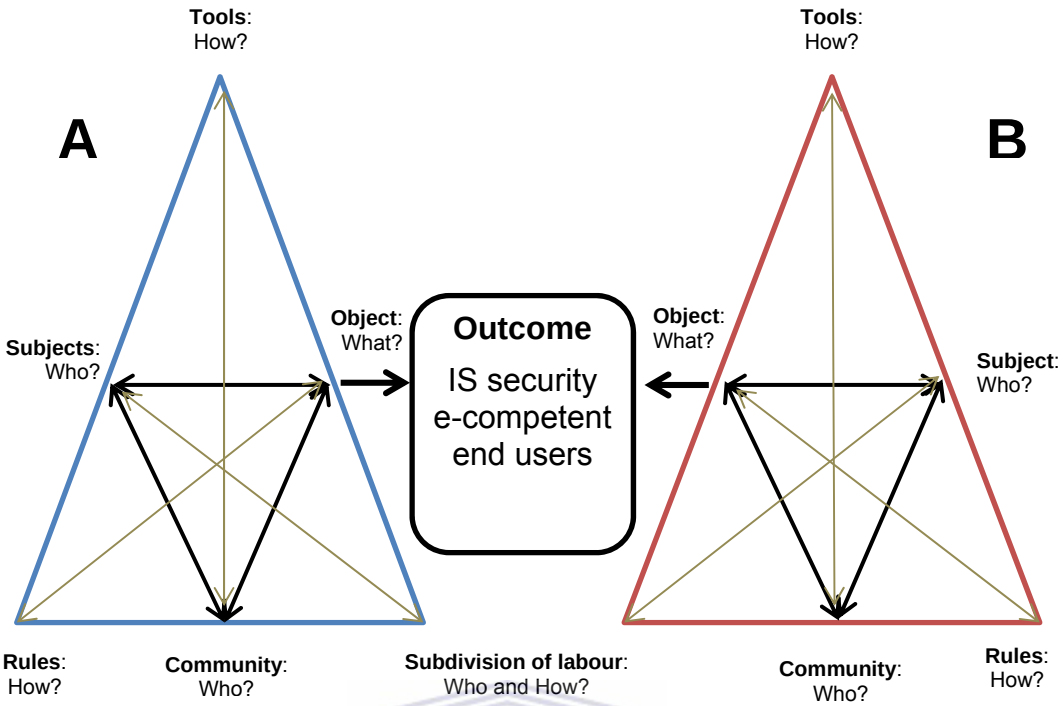


Figure 2.2: The IS security e-competencies development conceptualisation as Overarching Activity System (OAS)

Source: Adapted from Clark & Fournillier (2012); Allen et *al*. (2011) Paraskeva er *al*. (2010); Nardi (1996:29)

In the AT perspective, conflicting relationships between the constructs (i.e. subjects, tools, rules, community, and division of labour) of the system cause disruption instead of achieving the common outcome as the relationships are intended for (Allen, 2010). Thus, the object need to change because of changes and conflicts that occur in other constructs. In the context of this research, the IS security e-competencies can be successfully developed only if the constructs that render this development relate to each other appropriately. Otherwise there will not be a successful outcome. As an example, the negative participation of subjects (or policies preventing contract staff to participate in training), non-availability to tools, conflicting rules, non-supportive community or inappropriate separation of labour will all have a negative impact on the outcome of IS security e-competencies development.

As Figure 2.2 shows, on one hand there is an activity system (A) which presents the end users as the subjects separated by the different groupings according to the IS security e-competencies required in their jobs settings. In this case, their object is to become IS security e-competent. On the other hand, there is another activity system (B) with the suppliers of IS security e-competencies as its subjects and the object of supplying IS security e-competencies to end users. The two activity systems have common expectations, namely to have e-competent IS security end users. This is a deciding factor for the competencies at a specific level of employment.

The two activity systems are also related because they are regulated by common rules and operate in the same community. However, they are different in their subdivision of labour as some subjects act as suppliers and experts and others are recipients. In both systems, the subjects need to be conscious of their actions and activities with an objective to achieve an object that need to be transformed into an outcome that fulfils the purpose of the activity (Sun & Qu, 2014).

The successful achievement of the object of the activity (positive outcome) is possible only if each of the constructs is fully available and committed to the cause of the activity (IS security e-competencies development). Any non-alignment and unavailability, even in terms of quantity and quality of any of the constructs can result in the unsuccessful achievement of the outcome. If the elements comprised of the activity system or systems are fragmented, the achievement of the object becomes uncertain and confusing (Engeström, 2011).

2.3.5 Applying Activity Theory in other learning contexts

As a social theory, AT has recently been applied as a guideline or framework in various fields such as those related to the development of oil rigs, to women refugees, environmental studies, and education (Somekh & Lewin, 2005:188). This diversity of AT application is the main advantage of the approach as it considers the context of the activity (Allen et *al*., 2011) and does not offer a particular solution to a single domain. In other words, its cross-disciplinary application enables the adaptation to particular context (Stuart, 2014).

AT is also applied in learning and study activities in which IS was used as its core activity such as: for building adaptive e-learning systems (Peña-Ayala *et al*., 2014), tools for facilitating two instructors' interpretations for professional development (Clarke et *al*., 2012), re-conceptualisation of practice with multilingual children with speech sound disorders (Verdon et *al*., 2014), conceptualisation of learning through simulation (Berragan, 2013), mobile learning to assist individual knowledge management (Liaw, 2010), and the development of student teacher's creativity in design (Abdullah, 2014). AT was also used in the study of learning and other social interactions in museums and other similar setting contexts (Ash, 2014).

In the field of Information Systems, AT has been used to understand the human-computer interaction (Bertelsen & Bodker, 2003 cited in Bharosa et *al*., 2012).

From the above-mentioned researches in which AT was successfully applied, none of them was used to analyse the development of IS security e-competencies among end users in the HEI environment. In addition, neither of the studies applied the activity system as a theory for interpreting the interplay between the constructs in pursuit of the common outcome. Therefore this research presents a unique application of AT as it is not only helping with the analysis of IS security e-competencies development constructs and their influence on the object, but it is also taking account of the context in which the activity is taking place and the needs of individual subjects in the HE environment.

While AT can be used to study the development of IS security e-competencies among the employees in the HEI to strengthen their ability to secure the IS resources they access in their environment, it is not the only theory that can be applied for the development of e-competencies for end users. Thus, such a study can be perceived from different angles for example from a Human Resources (HR) development angle or a Human Capacity Theory (HCT) perspective. However, this research will not consider these angles, due to certain limitations.

2.4 CHAPTER SUMMARY

The development of IS security e-competencies in HE environment for the purpose of IS resources is a complex undertaking that can only be well understood through the application of socially oriented tools and techniques as the IS security e-competencies development activity is taking place in a social environment, in this case the HEI.

For the purpose of this research and the study of the IS security in the social environment such as in the HEI, Activity Theory (AT) and Human Capacity Theory (HCT) proved to be useful theories. By way of AT's Overarching Activity System (OAS) it is possible to have a comprehensive understanding of the constructs of the activity and their interaction in the achievement of the activity's object.

The analysis of IS security e-competencies development gives an understanding of the activity in a holistic and interpretive way through the use of the constructs as the AT provides. This is further possible, as the theory leads to the identification of subjects, an object, tools, and the social constructs that play a critical role in the development of IS security e-competencies. Through the application of AT principles, it was also discovered that the subjects that participate in the activity system need more than one action to achieve the object of an activity, and each action needs specific operations. These constructs of the activity system need not to be fragmented and confused, as this will lead to an uncertain and confusing object.

CHAPTER THREE: LITERATURE REVIEW – CONTEXTUALISING IS RESOURCES IN THE HIGHER EDUCATION CONTEXT

3.1 INTRODUCTION

Regardless of their industry and size, organisations and end users are faced with an old challenge of securing IS resources. The securing of IS resources has become difficult due to the dynamic and innovative nature of both the ICT industry and security threats. Because of the importance of IS resources in improving business operations, there is also an increased importance for their protection.

In the old days, the security of the IS (mostly manual) was made possible by physical security, lock, bars, and safes. Also, the attacker would travel to the organisation to commit the attack (Jones, 2009). The IS of the old days were more simple, as it was a single application on a single processor and non-shared database and memory, and were also not integrated (Fakeh et *al.*, 2012).

This comparison shows that the IS resources security techniques existed since the old age of manual information processing (Kouns & Minoli, 2010:21), but has evolved with the evolution of ICT and the threats affecting them. This evolution has created opportunities for business and attackers (Choo, 2011) as both parties have moved away from physically restricted locations to do business and t attack, to online business and online sophisticated and targeted attacks.

Today, while still recognising the importance of old protection measures, the interconnectedness and the sharing of information resources dictate an increased protection of the ICT assets against the multifaceted forms of threats and the risks from authorised and unauthorised end users (Williams, 2007). Thus, there is also increased need for protection of the IS resources that goes beyond the technological-focused controls.

As a result, this chapter provides answers to the importance of IS resources and their security in HEIs (Sub-question 1) and the identification of IS security e-competencies needed by IS resources end users (Sub-question 3). It also focuses

on the discussion of the practices of IS security in general. It starts with the identification of common IS resources and their security criteria, then a review of common threats and security measures related to IS resources, followed by a review of selected standards for IS security management, and concludes with a discussion of the impact of culture and legal regulations of IS security.

3.2 COMMON INFORMATION SYSTEMS (IS) RESOURCES AND THEIR SECURITY CRITERIA

This section identifies, categorises, and discusses the common IS resources that different end-users apply to access and process, as well as informs on the transmission of information in the HEI environment and the need for information protection. It also identifies the state (criteria) in which IS resources need to be maintained to ensure that they contribute to the achievement of business objectives.

3.2.1 Common Information Systems resources

There are different ways to categorise resources in the business environment. Apart from the accounting and business ways of identifying resources as tangible and intangible assets (Peng & Meyer, 2011:101), in ICT they are also identified as assets and include hardware, the media, the communication elements, and information assets (Kouns & Minoli, 2010:4). With precision, IT Governance Institute (2007), Davis et *al*. (2007:316-317) in the Control Objectives for Information and Related Technology (COBIT) 4.1 framework applications, and Monk & Wagner (2013:3) have identified information, infrastructure, and people as the key IS resources used in modern information systems to store, organise, process, and distribute information.

In this research, the discussion of IS resources are based on the following computer-based IS resources (Oz & Jones, 008:18); Gollmann, 2011:22-23); Turban & Volonino, 2012:8-9; and Rainer & Cegielski, 2013:12-13):

1. **Hardware**: is the different peripheral equipment categorised in input, processing, storage, and output hardware.

2. **Software**: includes programmes or set of programmes such as applications and system software.

3. **Databases**: is the collection of related files or tables that organise and store data for future processing and are created, maintained, and deleted by using the database management systems.

4. **People**: are IS professionals and non-professionals, managers or lower level employees, and general end users that access the IS resources to perform different tasks. For the professionals it is to design, construct, and maintain the systems while the non-professionals (general end users) access the IS to perform their tasks. In the case of HEIs, these tasks would be the capturing and processing of employee and students' information or the processing and distribution of financial information.

   As people (end users) are at the centre of this research, their skills, attitudes, perceptions, and personal agendas determine what they are able to do as part of ICT (Piccoli, 2012:31). With reference to security of IS resources, some of these attributes help them contribute positively or negatively to the protection of IS resources.

5. **Information and data**: Even though information and data are different concepts, they are both captured and stored and distributed through the use of IS resources. According to Rainer and Cegielski (2013:13) data are not organised to convey a specific meaning while information convey a specific meaning to the recipient. For the purpose of this research, they can be written or printed on paper, stored in digital form, transmitted by using post or by means of electronic systems; it can also be stored on movable devices or by using spoken words. In either of these forms, they are part of IS resources and need to be protected.

6. **Processes or procedures**: These are the set of instructions and rules on how the different IS resources collaborate (or are accessed) to process input through to output that satisfy the end users. In the HEI, there are processes related to the registration, payment of schools fees, ordering of stationeries and other resources, and those related to the security of IS resources.

7. **Telecommunications or networks**: These include the wire-line and wireless resources that facilitate the connection to the local and wide area networks for the sharing and transmission of data between the connected resources. In the HEI, resources such as printers and computer servers are commonly shared. They also help in accessing information worldwide in digital form (Ciampa, 2014:153) to facilitate teaching and learning.

Apart from the seven components of IS resources above-listed, Humphreys (2008) also identifies mobile devices such as laptops, cellular phones, flash memories, MP3 players (and audio recorders) as IS resources which can be used for the storing of sensitive information and can be accessed and used off-site. It can be used for insiders' private business, or it can be lost. In any case, the private use or loss of these resources can render the resources to be unavailable, which is a threat to the IS resources availability and breach of IS resources security.

The identification of these components is important in the sense that they work connectedly with each other to deliver the outcomes and people occupy the centre stage of the operations. With inference to the idea of Piccoli (2012:32) in relation to the interplay between the IS resources, Figure 3.1 illustrates that people (end users) are at the centre of the operation and protection of all IS resources.

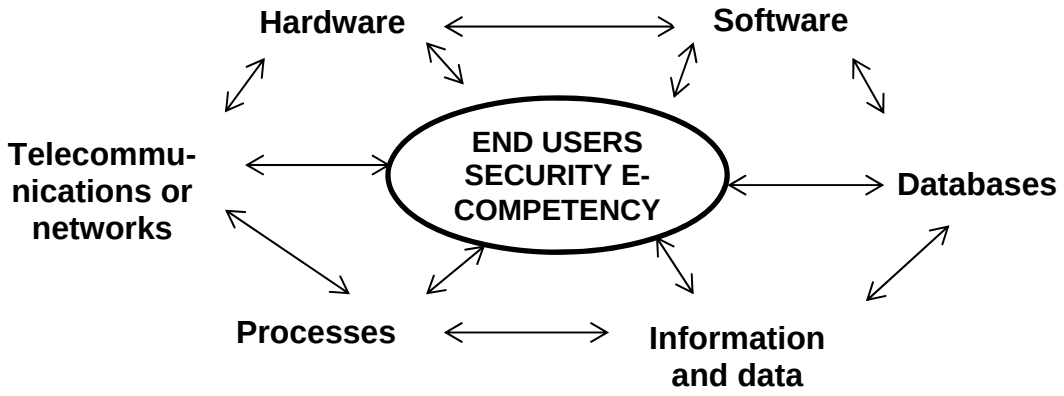


Figure 3.1: Effect of people security e-competency on other IS resources

(**Source**: Adapted from Piccoli, 2012:29-30)

Figure 3.1 signifies that the IS resources do not work in isolation, but interact with one another. It stresses that the level of IS security e-competencies of the end users, when using these resources, has an impact on the resources' protection.

Following the identification and description of the IS resources used in the HEI environment, the next section describes the (security) criteria of these IS resources.

3.2.2 Information and Information Systems resources criteria

In its recent publication, ISACA (2012) presents people and information as an organisational governance enabler. These are classified as resources at the same level as framework, principles, structures, processes and practices through, or towards which action is directed and objectives can be attained. In other words, without these resources (information that meet its criteria) HEIs cannot be able to create value and serve their purpose. To serve their purpose, information and other IS resources need to meet certain criteria that ensure that IS resources are ready to be used at the required time.

Even though the criteria of Davis et *al*. (2007:316-317) and Kouns & Minoli (2010:175-176) originally applied to information, in this research they are considered to be relevant and applicable to the security of other IS resources (Section 3.2.1). The following criteria are an extension to the ordinary confidentiality, integrity, and availability (CIA) triangle of IS security. The explanation of these criteria is based on the ideas of Ciampa (2014:12), Vacca (2009), Harwood (2011:9, 35, 345), Gollmann (2011:34-39), Jirasek (2012) and Farn et *al*. (2008):

- **Effectiveness**: This criterion requires the IS resources to produce a result that was intended. This can be applied to different resources, including the access and operability of IS resources in the HEI environment.

- **Efficiency**: The IS resources should at all times produce results with no or minimum waste of time, energy, or money. Or they should be made easy to use, backup, store, retrieve and maintain at no or minimum cost and time.

- **Integrity**: The IS resources (in soft or hard format) need to be kept in its desirable state as initially intended (Farn et *al*., 2008; Gollmann, 2011:35) and cannot be intentionally or accidentally altered (Holtsnider & Jaffe, 2007:352). The change or update needs only to happen through the formal process even though the authorised users steers it (Zafar, 2013).

  Information and other IS resources are complete and uncorrupted (Whitman & Mattord, 2010:6) and unauthorised people cannot alter it during processing and transmission. Access control can prevent the unauthorised access and ensure integrity of the IS resources in the HEI environment.

- **Reliability**: The IS resources should be able to provide intended result even in the case of extreme challenges and need to support the HEIs operations even during the extreme challenges. This refers to the need for robustness or duplication of IS resources and preventing (accidental) failure.

- **Availability**: The end users need to access the IS resources at the needed time without repudiation of services (accessed 24 hours a day). Also, access should be granted with reliability whenever authorised people request the resources (Farn et *al*., 2008; Zafar, 2013). This criterion applies the opposing position of the denial of service and is derived from the fault-tolerant computing environment (Gollmann, 2011:36).

- **Confidentiality**: This criterion requires that only authorised people in the HE can access the IS resources. Non-encryption of information traveling on network can create an opportunity for non-compliance with this criterion. Confidentiality combines security and secrecy of IS resources to prevent unauthorised users from accessing and reading the content of IS resources (Holtsnider & Jaffe, 2007:352; Farn et *al*., 2008; Gollmann, 2011:34). It includes also information, access classification, and secure documents storage (Whitman & Mattord, 2010:6) to ensure that personal information of students, employees, and other business partners are not disclosed.

- **Compliance**: The IS resources that the HEI maintains need to comply with organisational, governmental, and international best practices related to frameworks, processes, policies, and processes designed to ensure protection form threats and/or not becoming a liability for the HEI. The current compliance debate in South Africa is based on The Protection of Personal Information Act (POPI) which is intended to protect personal information collected and processed by organisations in the country (Refer to section 2.9 of this chapter for detailed information on POPI Act.)

In general, Gollmann (2011:34-36) refers to the above-createiria elements as the traditional areas of computer security, which are critical to the security of IS resources. Also, the non-compliance of IS resources to these standards has a significant impact on the specific IS resources' security, value, and usefulness in supporting HEIs' administration and service delivery. This means that the decisions of HEIs (from registration of students and hiring of employees to graduation and retirement) depend on the good quality of information at the disposition of decision-makers which again depend on the quality of information transmitted through the IS resources they hold.

Actions such as denial of service (DoS) by flooding users with messages, lack of encryption (Harwood, 2011:345), not locking of office premises, or non-protection of IS resources against unauthorised access, at most affect most of the criteria of IS resources.

Therefore, the protection of information by insuring that the listed criteria are maintained also apply to all the other IS resources used in the process of collection, storage, processing, and distribution of the information. Since, when IS resources are affected, the information is also affected (Ciampa, 2014:12).

3.3 INFORMATION SYSTEMS – THREATS AND SECURITY MEASURES

The current knowledge-economy is based on the interconnection and interchange of data among functional areas within an organisation or between business partners as opposed to old silos departmentalisation (Monk & Wagner, 2013:14) and isolation

among business partners. In this situation, the security challenges arise which requires the protection mechanisms to protect the system from its users, and users from each other (Gollmann, 2011:2).

Especially with the advent of online transactions, e-learning, central management of IS resources in common databases, the security of IS resources have also attracted the attention of many people for both good and poor reasons. Hence, the following sections discuss general threats to IS resources and common security mechanisms applied to protect the IS resources.

3.3.1 Common sources of threats to Information Systems

Organisations and HEIs face a rising of threats to IS resources and perpetrators are become more ingenious daily (Lynn, 2009; Doherty et *al*., 2009; Williams, 2012). It is known that these threats and other disruptions to normal business operations have cost organisations an estimated amount of R57.8 million of losses annually (Stander et *al*., 2009). According to a research cby Penemon Institute and Symantec Research presented in Ciampa (2014:4), the average cost of a single data breach to a business is about $7.2 million.

The threats themselves originate from traditional, mobile, and digital environment sources. This is why organisations need to apply various security measures to protect these IS resources.

In this regard, Ciampa (2014:38,78) asserts that, early threats were intended to cause vandalism, focusing on the erasing of files and data, corrupting hard drives to prevent end users from accessing the IS resources, slow down computer performance, and even to display provoking messages. Although the older objectives still exist, the focus has also moved to the stealing of data for financial gain.

3.3.1.1 Internal threats

The internal threats refers to those committed by insiders who have right to access the IS resources (employees, consultants, janitors and guards). The internal security

threats can be categorised into intentional malicious behaviour and unintentional behaviour or those due to carelessness behaviour of staff members.

The intentional threats are associated with disgruntled or ill-willed employees. It is difficult to prepare for these threats as they are committed by trusted people who commit unauthorised acts such as the selling of customers' information or installing security threatening devices or applications.

Signalling how enormous the insiders' threats are to the IS resources of any organisation, Colwill (2008), Crossler et *al*. (2013), and Richardson (2011) confirm that more than 50% of fraud is perpetrated by insiders rather than by external criminals. The fact that worsen the case is that organisations, in their responses to security threats, focus 90% of IS resources protection on external threats with technological controls (Vroom & Solms, 2004; Colwill, 2009).

In line with the above statements, the world witnessed the case of Edward Snowden who was contracted to work for the U.S. National Security Agency (NSA) and then leaked the classified information of his employer in June 2013. Since, the U.S. Government has charged him with various criminal offenses. Ciampa (2014:21) confirms that insiders' attacks are mostly sabotage and theft of intellectual property, mainly by employees who are disgruntled, those resigning, demoted, or fired.

Other category of threats to IS resources falling under the category of human error include (Sarkar, 2010; Piccoli, 2012:389; Rainer & Cegielski, 2013:86-87):

- Carelessness with computing devices in the office or public places;
- Opening questionable e-mails and breaking the organisation's policy on Internet and Web usage;
- Failing to modify default password and poor password selection (or re-use of the same password on different systems (Furnell & Moore, 2014)). In fact, the password itself has become easy to break and no longer considered as a strong security measure on its own (Ciampa: 2014:40);
- Carelessness in monitoring environmental hazards such as dirt, dust, humidity, and static electricity which are harmful to IS resources;

- Social engineering which uses social skills and psychological techniques to trick legitimate employees to provide confidential information such as passwords. It can be perpetrated through tailgating, shoulder surfing, dumpster diving, desktop snooping, impersonation, and the model that combines any of these models (Ciampa, 2014:44-45; Sarkar, 2010).

  According to Okenyi & Owens (2007), social engineering, which is part of human hacking, can be human or technology based. The technology based uses technology (computer applications) to retrieve information from individuals in the form of phishing attacks.

Furthermore, Rainer & Cegielski (2013:85) and Sarkar (2010) state that human errors or mistakes by employees pose a large problem as the result of laziness, carelessness, improper training, and lack of awareness concerning information security from both management and end users (Rhee et *al*., 2012; Whitman & Mattord, 2010:57). This lack of awareness stems from inadequate training by the organisation (which is also a weakness in security e-competencies). The danger to the organisation due to the lower level of IS security e-competencies present a threat to IS resources security which is bypassed or modified (Fischer et *al*., 2012) without knowledge of end users as they themselves are not aware of their correct state.

These unintentional acts suggest that the "security posture depends on appropriate end user behaviour" and other factors (Rhee et *al*., 2009 and Furnell & Rajendran, 2012). This is beside the implemented security layer to protect IS resources. If the end users do not keep passwords confidential and cannot protect themselves against the social engineering manipulations, or change their internet surfing habits, cannot update the passwords or set up the firewall correctly, the IS resources they access could be negatively impacted.

3.3.1.2 The external threats

Piccoli (2012:389) stipulates that people outside the organisation are responsible for the **external threats.** These people are mostly crackers, thieves, social engineers,

and industrial espionage contractors who profit from the pervasiveness of networking and Internet to attack organisations. The mostly use security threats such as:

- **Intrusion** threats to get access to IS resources without authorisation;
- **Social engineering** which even if it succeeds because of human error or lack of awareness; it is committed by external people who try by all means of deception to get access to IS resources;
- **Phishing attacks** which consist of sending deceiving and unwanted e-mails (spams) with request of sensitive personal or organisational information;
- **Exploitation of backdoors** and security weaknesses known in some commercial applications that allow access to the application through circumventing the password protection in the case of inaccessibility of a high-level account. While some backdoors are locked during the installation process, sometimes the process is forgotten and allows the access into the application while it is operational;
- **Trojan and malicious codes** or malware such as viruses, Trojan horses, worms, and spyware which are designed to cause damage to IS resources;
- **Denial-of-service** attacks which are intensive given the predominance of online operations. It is a digital assault which is directed to online service over the network to force it offline;
- **Keylogger**, which can be a small hardware or software and can be undetected that connects to the back of the computer in the form of an USB connection, external devices like a keyboard and then used to collect keystrokes as they are punched by end users (Ciampa, 2014:82-83).

Apart from the technological threats, Rainer & Cegielski (2013:85) recognise the importance of other threats to IS resources that are not related to technology but still threaten the integrity of IS resources. These include natural disasters such as floods and storms and man-made disasters such as fire, power outages, and other related incidents. In these cases, organisations may be required to get insurance in case other controls cannot eradicate the problem.

As part of IS resources security e-competencies, it is also important to identify the specific threats that affect IS resources at different processing stages (Harwood,

2011:104-120; Zhang, et *al*., 2010; Alebrahim et *al*., 2014; Baldini, 2012) and identify also appropriate controls to manage the threats. Table 3.1 [summarised from Piccoli (2012:388-400) and Rainer & Cegielski (2013:83-103)] identifies the sources of threats and the security measures that can be implemented to control the threats.

Table 3.1: Summary of threats to IS resources and related security measures

SOURCES OF THREATS	SECURITY RESPONSE MEASURES
Internal threats (generated by trusted employees)	Mostly dealt with through the security policy (Piccoli, 2012:395) which articulates the behaviour of staff and separation of IS resources that are made available to different categories of employees. The format of password and related rules, data access, download, and transfer format. Internet and e-mail principles. Audit review and compliance. And other aspects of IS security as the organisation deems important.
External threats (generated by people external to the organisation)	There are the basic security measures such as password and encryption to prevent intrusion and unauthorised access, firewall to control traffic, security policy and audits to block backdoors. Piccoli (2012:395-398) suggests training policy, antiviruses, and spyware sweepers to prevent safeguards against malware. Rainer & Cegielski (2013:94-103) introduce three categories control measures (known as counter-measures) to protect all components of IS resources which are briefly described in the following paragraphs.

To conclude this section on threats to IS resources, it is important to know that in all cases, damage is real - be it intentional or unintentional, internal or external, the committed incident can result in the damage to the organisation, loss of business, loss of competitiveness, negative media publicity, loss of credibility and reputation, fines and even law suits because of the deliberate or accidental disclosure of business partners' information (Crossler et *al*., 2013; Bhargav & Kumar, 2011:22; Okenyi & Owens, 2007; Townsend & Bennett, 2003 as cited in Zafar, 2013).

To follow this in-depth discussion of IS security threats and security measures that protect IS resources, Section 3.4 below debates some of the security standards that

are applied as best practices for implementing and managing IS security in the organisation.

3.4 ICT SECURITY MODEL AND STANDARDS

The term ICT security model refers to a “generic security blueprint offered by a service organisation” (Acevedo, 2012:242). In ICT security, it provides a detailed outline (Whitman & Mattord, 2014:212-213) to be followed in the design, selection, and implementation of security controls, policies, training and education.

Models and standards can be adopted and modified to meet the IS security needs in the HE environment and to serve as a starting point for adoption and implementation of policies, hardware and software or the combination of both (Whitman & Mattord, 2014:212, 219). The application of these best practices “demonstrate the HEI commitment to secure business practices and may be used to apply for certification and accreditation” (Siponen & Willison, 2009).

The discussion of the security models and standards in the following section is focused on defense-in-depth model and the International Organisation for Standardisation ISO 17799/27002 frameworks. These are generic in scope and can be adapted as best practices in IS security in any industry or organisation of any size (Siponen & Willison, 2009; Humphreys, 2008) including the HEI.

3.4.1 The IS security defense-in-depth model

Since Turban & Volonino’s (2012:131) proposal of the IS security defense-in-depth model many organisations across the globe, including the U.S. Department of Defense (DoD), adopted the model for their own purposes. Figure 3.2 illustrates the defense-in-depth model.

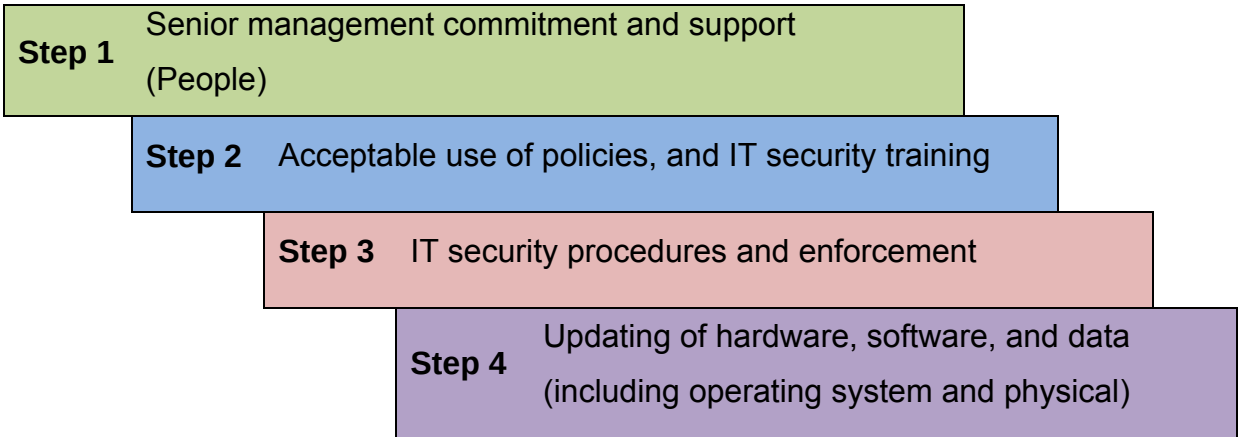


Figure 3.2: IS security defense-in-depth model

(**Source**: Adapted from Ciampa, 2014:13; Turban & Volonino, 2012:131; Bhargav & Kumar, 2011:27)

Figure 3.2 presents a comprehensive approach to IS security needs. It is illustrated as a multi-layered approach in which one layer provides security to IS resources in case another fails and it involves people, processes, and technology (Bhargav & Kumar, 2011:35-36; Herath & Rao, 2009; Turban & Volonino, 2012:130). Such holistic approaches are in demand for IS security to view technological security from a broader perspective (Faris et *al*., 2014), but with specific focus on human IS security e-competencies at the centre of all the other activities.

The security model (Figure 3.2) helps in explaining the importance of a multi-layered approach to IS security (Jirasek, 2012) and places end users in the security of IS resources. Other aspects related to information security according to the model are:

- The success with IS resources security depends on the executive management, technical security staff, and end users involvement (and skills level) as well as commitment in the process through ethical standards, privacy control, and internal control;
- The second step is related to the development of acceptable custom policies and training users in security related policies to ensure that they know their roles and responsibilities;
- The security procedures and enforcement should ensure the monitoring and compliance to acceptable user policy (AUP); and

- The implementation of hardware and software is an important step to support the policies and to secure practices.

The model (illustrated in Figure 3.2) also confirms the Sarkar's (2010) view that insider threats are "fundamentally a people issue." As such, technological controls alone cannot be sufficient to control (Ciampa, 2014:88; Herath & Rao, 2009). They may be applicable in reducing threats related to access control, monitoring identity threats, but has to be run concurrently with organisational and behavioural controls to be effective. As such, the inclusion of human behaviour in the security programme requires training and development of end users on IS resources security which are directed through the institution's policies. Otherwise, the development of competencies cannot be achieved.

3.4.2 The International Organisation for Standardisation – ISO 27001 and ISO 27002

Despite the uniqueness of organisations and their exposure to IS security threats, there are common approaches and standards (Kouns & Minoli, 2010:73) that are applicable to all organisations. Such standards include the ISO 27001 and ISO 27002 which are internationally recognised guidelines that address how IS security should be addressed in an organisational setting.

The adoption of a security standard provides an organisation with a bench mark and best practice to audit and monitor its own IS security practices against the best practices included in the standard (Broderick, 2006). In the case of the ISO standards, HEIs can use only those relevant controls applicable in its situation.

The two standards (ISO 27001 and ISO 27002) are closely related. ISO 27001 acts as a standard for ICT security and defines a set of requirements which can be used for certification. ISO 27002 contains a set of best practices and guides in form of control objectives and controls that can be used for building security architecture even if the organisation does not seek a certification (Hayden, 2010:224-225).

While in the process of writing this research, the new ISO 27001:2013 and ISO 27002:2013 had just been published, and show improvements in areas such as (PR Newswire, 2013):

- Incorporation of feedback from practitioners and simplification for integration with other management systems; and
- The standards have been made easy for customers to use and address new and existing security needs.

2.4.3.1 Controls and focus of ISO 27002

The current version, the ISO/IEC 27002:2013 standard has evolved from its predecessor ISO 27002:2005 standard which was also a development from the ISO/IEC 17799:2005 and former BS7799 developed by the UK Department of Trade and industry (Siponen & Willison, 2009) in the early 1990s for the management of information security (Broderick, 2006; Humphreys, 2008).

The ISO 27002 provides guidance for best practices in security management for organisations (Ahmad et *al*., 2014). It is not a technical standard for security products or a set of evaluation criteria for IS security (Gollmann, 2011:19). As other generic best practice standards, it highlights the key aspects of IS security that should be considered to ensure that the IS resources are protected from threats.

Kawasaki & Hiromatsu (2014) states that the ISO/IEC 27002:2013 has fourteen clauses that represent 113 security controls, all of which are generic objectives of ICT security, opposed to the twelve of a its predecessor (Kouns & Minoli, 2010:8; Gollmann, 2011:19-21; Humphreys, 2008):

1. **Security policy**: refers to the clause that contains two controls that can provide direction and support on any security matters in the higher education environment.

   For any organisation relying on IS resources and the Internet to provide services to its customers, it is important to highlight the importance of ICT security policy. Gollmann (2011:41) and Reynolds (2012:105-106) suggest that security policy defines those security requirements and those controls

needed to meet the requirements. It also regulates the relationship between the users (subjects) and the IS resources (tools), and highlights the key resources in which security mechanisms are implemented. It outlines what needs to be done but not how to do it. Security policy comes to help in informing users about their responsibilities in relation to IS resources (including Internet and e-mail), preventing misuse and reduce exposure and legal liabilties (Turban & Volonino, 2012:131).

2. **Organisation of information security**: This clause contains seven controls that address the organisational structure, responsibilities and reporting structure to facilitate the communication and implementation of security related decisions.

3. **Organisational asset management**: The clause contains 10 controls and ensures the analysis and classification of ICT assets and their values to ensure that the asset value and the cost of security are in balance.

4. **Human resource security (personnel)**: This clause holds seven controls and stresses the importance of understanding that the organisational employees or contractors can be a source of threat or insecurity to the IS resources. Measures should be in place for employees that either join or leave the organisation. It is important to identify employees who collect the keys and badges, delete accounts of users leaving the organisation, and ensuring proper background checks on newly hired staff members.

5. **Physical and environmental security**: The clause covers 15 controls related to the environment in which IS resources can be the weakest link in the chain (Bulgurcu et *al*., 2010). Therefore, measures such as fences, locked doors, protection of sensitive areas and rooms need to be enforced to prevent unauthorised access to IS resources to prevent damage or theft of these resources. Natural disasters (weather condition and possible flooding or fire) also need to be referenced when dealing with this component.

6. **Communications Security (network security)**: This component addresses the day-to-day running of IS resources, both transmitting resources (hardware and software) and transmitted resources (information when stored, being processed, or being transmitted) to ensure that their security is maintained on the network through encryption and by the end users through policies.

7. **Access control**: The clause encloses 14 controls that address questions like identifying the authorised person to access the IS resources (data, information, hardware and software, network resources, documentations). Given the advanced degree of digitisation, particular attention needs to be given to remote access in IS resources.

8. **System acquisition, development, and maintenance**: The clause holds 13 controls and requires that the security of IS resources be maintained during each stage of the system development lifecycle. Including fixing discovered vulnerability in coding, upgrading of antiviruses as well as providing support to end-users in requests and issues such as forgotten password and Internet connection.

9. **Information security incident management**: This clause contains seven controls and it deals with the organisation of ICT structure in terms of reporting and responding to security threats if the organisation is affected. This component also includes instruction to users in case of unusual issues.

10. **Business continuity management**: This clause comprises four controls and it addresses issues like backup of data stored in different locations, the creation of hot (or warm and cold) sites that can be used while the operations on original sites are being restored, and also having measures to ensure that operations continue even in case of sudden loss of key staff members. All these actions are considered to ensure that the HEI continues its operations even during the time of disaster and failure of critical resources.

11. **Compliance:** This clause contains eight controls related to how IS resources are developed and managed to comply with rules and standards specific to certain industries or general to all industries for standardisation purposes.

Aspects such as those related to legal, regulations, general ICT and security standards, and organisational policies are among the requirements that IS security needs to comply with.

12. **Supplier relationship security:** The clause covers five controls that deal with security information and the contractual relationship with external suppliers of products and services. The emphasis is placed on monitoring, auditing, and control of the contract and service level as well as how to ensure awareness on policies and procedures for IT resources security.

13. **Cryptography:** The clause encompasses two controls and ensures that the organisation has a control on encryption, digital signature, and the management of encryption process and keys used during the encryption.

14. **Operations security:** This clause involves 14 controls and ensures that the organisation applies proper and documented procedures at all times during IT operations. Aspects such as end user awareness on IT resources security, control on the installation of software, planned audit and proper repairing of vulnerabilities and backup processes are to be addressed.

The above topics can be classified in three categories of IS security. Tshinu (2007), taken from Callio Technologies (2007), summarise it in the following ways:

- The first category addresses the **organisational** aspects of IS security; and includes security policy, asset management, compliance, human resource security, and business continuity management;
- The second category addresses the **technological** aspect of ICT security; which bring in access control, Information systems acquisition, development, and maintenance, Communication and operations management, and information security incident management; and
- The third category addresses the **physical** aspects of IS security to incorporate the physical and environmental security.

2.4.3.2 ISO 27001 process for information security

As with its predecessor BS7799 and ISO/IEC 27001:2005, the ISO 27001:2013 standard is the auditing and certification standard for IS security version of ISO 27002:2005 (Ahmad et *al*., 2014; Eminağaoğlu, et *al*., 2009; Louns & Minoli, 2010:75). According to Louns & Minoli (2010:75), the standard specifies a set of requirements for the establishment, implementation, monitoring and review, maintenance and improvement of an Information Security Management System (ISMS) in the organisation. It also provides security controls from which organisations can seek certification for their ISMS from.

The standard uses the Plan-Do-Check-Act (PDCA) process on the information security guideline. Whitman & Mattord (2010:226-228) and Siponen & Willson (2009) explain the process:

- Plan: Includes the establishment of security policy, security controls, procedures, assess risks, and the scope of their establishment.
- Do: Formulate the risk treatment plan, implement the identified security policy, controls, manage operations and resources, and implement procedures to detect or respond to security incidents.
- Check: Assess the performance of the implemented solutions and report on their performance (review of implemented procedures and residual risks).
- Act: Take the corrective actions if there is a gap between the result and the intent degree of protection, communicate results, and apply the lessons learned to other situations.

The above process is often presented in the form of a cycle for the information security process model (Humphreys, 2008) and presented in Figure 3.3 below.

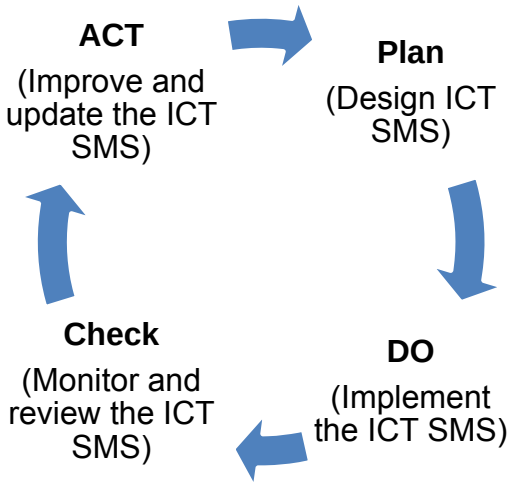


Figure 3.3: ICT Security Management System (ISMS) process model

(**Source**: Adapted from Whitman & Mattord, 2010:226; and Humphreys, 2008)

In relation to the process in Figure 3.3, Eminağaoğlu, et *al*. (2009) assure that within "any information security programme, it is important to audit, check and measure what is done to guarantee that efficient and effective security measures are implemented to protect IS resources of the organisation".

ISO 27001 and ISO 27002 complement each other, the former provides specification for information security management and the latter support the code of practice for the implementation of ISO 27001:2005 (Humphreys, 2008) and has 133 defined controls for security management (Ahmad et *al*., 2014 and Broderick, 2006). The new framework has 114 controls (Faris et *al*., 2014) of which the following are crucial according to Sedinić et *al*. (2014):

- A5: Information security policies;
- A6: Organisation of information security;
- A7: Human resource security;
- A8: Asset management;
- A9: Access control;
- A10: Cryptography;
- A11: Physical and environmental security;
- A12: Operations security;
- A13: Communications security;

- A14: System acquisition, development and maintenance;
- A15: Supplier relationships;
- A16: Information security incident management; and
- A17: Information security aspects of business continuity management.

Concerning this research, the controls A7: Human resource security, specifically through the security aspects related to controls such as physical and environmental security, and A9: Access controls were considered to highlight security e-competencies to be supplied to end users. These controls need to be included in the security e-competencies development as the end users have access to various IS resources that need to maintain their confidentiality, integrity, and availability that cannot be compromised.

In relation to security e-competencies development, the ISO 27002:2013 and its predecessors do not provide any details as to what these security e-competencies are, at which level they can be provided, and how they can be supplied in the context of HEI environment. It only provides a brief guideline on human resource security which addresses the employees' security clearance before and after employment in an organisation.

The importance of the ISO 27001 is that it assists in providing a holistic and flexible approach for managing IS security as it addresses issues such as people, process, legal, and IS resources (Humphreys, 2008). However, these issues are not specific to any organisation as the model is generic in nature and are just guidelines.

3.5 LITERATURE REVIEW ON IS RESOURCES SECURITY

From previous research on IS security, the following findings informed the foundation and direction of this research.

The imbalance between high investment in security technologies and low investment in security training, education, and awareness programmes (Wiant, 2005) creates a perception that one is more important than another. Yet, the impact of security

breach perpetrated against the IS resources through employees weaknesses affect the organisation to the same or even greater degree than a technological breach.

Siponen & Willison (2009) caution that “the mere existence of security practice such as policies and education programmes do not guarantee their quality practice”. These practices need to be actively operational and employees should be made aware of them. Continuous updating and or empowering of employees with proper security training is necessary to enable the installation of security technology (firewalls, antiviruses, intrusion detection systems, etc.) and the identification of security threats as well as to ensure maintenance in this regard (Smith, 2004).

In their study on e-Taiwan information system security, Farn et *al*. (2008) point to the protection of IS resources “through information assurance (IA) that addresses the full suite of security requirements for today’s information infrastructure”. This form of integrated information infrastructure security relies on people, the operations, and technology to which policies and procedural mechanisms at all layers throughout the organisation are combined to achieve the mission of the business and IS infrastructures management (Frederick, 2002 as cited by Farn et *al*., 2008).

Smith (2004) highlights the same perspective of integrated approach to the security of IS resources in his study on e-security issues and policy development. The author discovered, that security policy, management support, budget for security, and employees were components (amongst others) that helped achieved security of IS resources. In regard to this research, they support also the development of IS security e-competencies.

The mentioned form of integrated security structure addresses the security of IS resources in a holistic approach as opposed to the implementation of perimeter defences that protects the IS resources from outside threats alone, ignoring the insiders’ perpetrated threats which also cause significant damage to the availability of IS resources (Vroom & Solms, 2004; Sarkar, 2011).

Given their knowledge of the system, processes, location of critical and valuable assets, and privilege to access these systems, insiders' threats are more dangerous than outsider threats as they "are not just centred on technical vulnerabilities". Also, insiders "know how to cover their tracks" after the attack (Sarkar, 2011; Colwill, 2009). Similarly, no system can challenge an end user who has the correct information to access the system (Hinde, 2003 as cited by Williams, 2008).

To emphasise the impact on the insiders' threats to IS resources security, Colwill (2009) added that non-malicious threats can also result in major and a negative impact on the organisation. These include accidental loss or release of information to unintended users and carelessness with IS resources (such as leaving your laptop or external driver behind in a public place) by trusted end users. Even the most effective security technologies can still succumb to human failures (Rhee et *al*., 2009).

For explanation purpose, Humphreys (2008) says that it is employees or contractors at different levels in the organisation structure that commit insider threats. From those sitting on board, ICT security technicians, even those at the lower level of structure for various reasons, some steal IS resources (including information) for personal gain and others for sabotage and still others just because of human errors.

Jones (2009) writes on the factors contributing to the lack of awareness to risks on IS security, which include the lack of awareness on the working of digital information stored on digital resources. The author suggests that end users do not know that deleted information can be recovered by the use of trivial and easily accessible tools. This is another area that required security e-competency development at the relevant level that this research seeks to address through security e-competencies development.

Concerning the control of insider threats, Sarkar (2010) recommends that "*technologies can drastically reduce the insider threat problem but if it is concurrent with non-technological measures*". The two categories of recommendations are:

- Among the technological recommendations the suggested strong password policies, audit logs, authentication and encryption policies of sensitive data combined, and policies related to internet, free webmail, or e-mails, but also policies related to the deactivation of terminated employees accounts; and
- On non-technological recommendations the author suggested amongst other measures, to include the means for employees to report suspicious activities, introduction of regular security awareness programmes to all staff, easily comprehensive policies that are enforced, and regularly updated.

The study and integration of IS security in the organisation has not been an easy undertaking nor totally supported by all the end users in the organisation for various reasons. One reason proves to be that end users view security "*as a nuisance that is being forced on them to suffer*" (Furnell, 2009). This is with reference to end users being subjected to tight security check, online monitoring, security cameras, and required to follow the security policy in their undertakings.

Previous researches on IS resources security, strong recommendation is made that both technological and non-technological security measures should address the security of IS resources in an organisation (Sedinić et *al*., 2014, Bulgurcu et *al*., 2010). The shortcoming regarding non-security measures is that there is no clear specification of which security e-competencies need to be developed among the end user in the HEI and at which level of employment.

Therefore this research created a conceptual framework that can guide the HEIs in the identification and supply of needed security e-competencies for their end users to protect the IS resources they access to perform their daily activities.

3.6 IS RESOURCES SECURITY AND ORGANISATIONAL CULTURE

Apart from the focus on technological controls and the indoctrination of end users in IS security, the protection of IS resources in HEI, as in other business organisations, depends on the IS security culture in the organisation.

From a behavioural perspective, Schermerhorn et *al*. (2012:40) define culture as "the learned and shared way of doing things in a particular society". Daft et *al*. (2010:20) and Thomson & Solms (2006) say that culture represents the underlying beliefs, values and norms that the members of an organisation share, which are carried from one generation to another and inform the practices in the society. An example is the way members of the society dress, greet, and treat one another.

An organisation's culture is unwritten but can be observed in its stories, slogans, ceremonies, dress, and office layout (Daft et *al*., 2010:20). As such, the culture portrays to the external world what the organisation is and believes concerning certain issues such as IS security practices and IS security e-competencies development. In this regard, the organisation's IS security culture, if well aligned to its security policy and objective, can help shape the end users perception and behaviour toward IS resources security. Such thinking could also create an interactive bond as Figure 3.4 illustrates.

Figure 3.4 below, introduces an improved way to align employees' behaviour to IS security. It emphasises to understand and align employees to the organisational IS security practices and policy. One example is that when it is stated that employees are important and crucial in securing IS resources, it should be made visible through concrete actions like continual training and awareness on IS security; otherwise there is incongruence in the alignment.

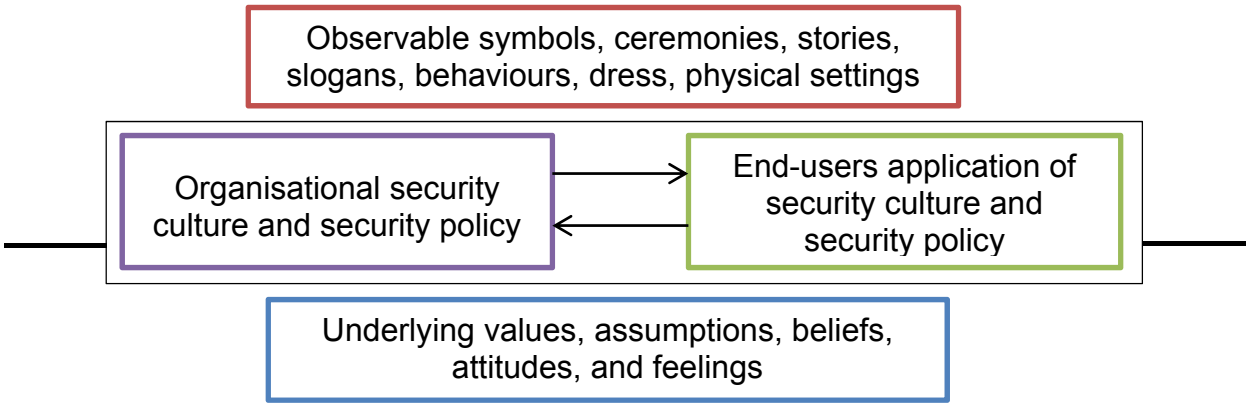


Figure 3.4: Organisational and end users security culture and policy bond

(**Source**: Adapted from Daft et *al*., 2010:400; and Vroom & Solms, 2004)

Security of IS resources is a multi-facet system that work well only if all the components of the system operate in a collective unity. The reality is, security technologies (hardware and software) means nothing if end users do not practice cyber safety (Lynn, 2009) or take care of IS resources. The best way to get end users to think and act about IS resources security is to create an on-going culture of security in the organisation (Colwill, 2009). The culture will have an influence on employees' "*behaviour toward IS resources security*" (Furnell & Rajendran, 2012).

Explaining the issue mentioned in the above statement by Colwill with security of IS resources in terms of non-technological measures is not only to provide training and awareness to end users, but integrating end users, their buy-in, and behaviour to the cultural values of the organisation in the protection of IS resources.

Literature does not indicate in a clear-cut way which culture to be the most appropriate to be integrated for the protection of IS resources. However, the following are among those identified aspects of IS security culture to be included:

- Making security training and awareness to be part of employees' job requirement by ensuring that no one can plead ignorance of security rules and rewarding of good security behaviour among the end users (Colwill, 2009). The way in which security issues are addressed (Williams, 2008) by the executives at all levels of the organisation. With reference to Leach (2003), the way executives and peers act with relation to security issues, has a direct impact on the behaviour of other employees in the organisation. Therefore, the actions and behaviour of executives dictate to other employees what the culture of the organisation is with reference to security culture and this serves as a guiding standard for the new employees in the organisation.

- The enactment of security at the executive management level of the organisation, so that the leaders can serve as role models for IS security to other stakeholders and help in integrating IS security into the functions of the organisation (Okenyi & Owens, 2007). IS security should not just be placed as an add-on activity (Smith 2004) and be dealt as time allows.

- Funding for security to be considered as part of business costs rather than discretionary costs which can or cannot be allowed (Okenyi & Owens, 2007).

Hayden (2014:6) asserts that "*even armed with the information and the skills, people still do not use what they know and do what they know how to do, because behaviour is significantly influenced by culture*". In relation to IS resources security, this means that culture needs to be considered as a driver of attitude, reaction and actions of management as well as a driver of end users, of which the purpose is to adapt and comply with IS security in the HEI environment like in other organisations (Thomson & von Solms, 2006).

In their study on information security culture, van Niekerk & von Solms (2010) discovered that effective security culture should include the interaction and alignment between the identified four levels (artefacts, espoused values, shared tacit assumptions, and knowledge). These cannot be created and installed as software, but it is "*intentionally shaped and directed through the change of a mind-set and attitude*" of the organisation's stakeholders. This process needs strong support from senior management (Sedinić et *al*., 2014). This change can be made possible in the IS security e-competencies development through education, training, and awareness campaigns (Sedinić et *al*., 2014) as is in the case of this research project.

Finally, unlike Sedinić et *al*. (2014) who argue that some organisations, like banks and intelligence services, require a strict security culture, this research debates that the implication for regulations and acts, such as the POPI act in South Africa, require all organisations (including HEIs) that collect and process information of customers, to have strict IS security measures.

3.7 IS RESOURCES SECURITY AND LEGAL REQUIREMENTS

Throughout its operations, HEIs collect, process, and disseminate information through the use of various IS resources to achieve their objectives. Given the importance and sensitivity of information that is collected, processed, and transmitted over the IS infrastructure to business and stakeholders, there has been also a rise in the abuse, misappropriation and unintended use from the part of both

authorised users and unauthorised criminals who access the IS resources illegally. The reason for these users and/or criminals to access the IS resources varies from being to collect the data (information) for illegal activities, cause panic, provoke catastrophe to the aim for financial gain (Ciampa, 2014:18; Yoon & Kim, 2013; Bhargav & Kumar, 2011:20).

The above misuse of data and information have forced governments and IT managers across the globe to regulate the collection, processing, and transmission of information and the IS resources through laws and regulations, and ethical standards to avoid liabilities relevant to misuse of IS resources (Whitman & Mattord, 2010:428). These laws and regulations act as guidelines and non-technological security enforcement measures to IS resources and information against any form of abuse, and criminal activities perpetrated against IS resources to protect the organisation, its stakeholders, and the country as a whole.

In South Africa, legislations such as the Promotion of Access to Information Act (PAI), 2000, the Protection of Personal Information Act (POPI) 2013, and the Electronic Communications and Transactions Act, 2002 are to regulate the collection, protection, access, and distribution of information in both digital and non-digital form by public and private organisations, including the HEIs. In this regard, the security of IS resources and of information is maintained not only with technical resources, but also through the application of legal regulations. Hence, the IS resources security has become a national government concern that requires official regulations and part of national security (Hayden, 2010:272).

In this research, the three Acts that the South African Government ordained that relate to the security of information have been briefly discussed. The full details of these Acts are presented in Appendix D:

- The Protection of Personal Information (POPI) Act of 2013.
- The Promotion of Access to Information (PAI) of 2000.
- The Electronic Communications and Transactions (ECT) Acts of.

3.8.4 IS resources security e-competencies development and legal implication (Acts) in Higher Education (HE) environment

All three Acts discussed in the previous section require a responsible party or their operators to *"treat any personal information which comes to their knowledge as confidential and must not disclose it*" in an unreasonable and unlawful way, as such behaviour will result in penalties (fines and imprisonment) associated to the unlawful disclosure. This forms a sufficient foundation for HEIs to be conversant and comply with.

Furthermore, since HEIs collect some sensitive information about third parties, conduct their own research and/or research in collaboration with business partners, or conduct research on behalf of third parties, it is imperative that all the stakeholders in the HE environment become familiar with these legal requirements. Familiarising of the legal requirements is essential to prevent the institution from being prosecuted or fined due to non-compliance to the National Laws that govern the processing of personal information.

Therefore, preventing carelessness when handling personal information and IS resources that collect, store, process, and distribute information is beneficial to HEIs and improves the services to its stakeholders. This can be done through training and awareness about legal requirements of information and IS resources (development of security e-competencies) among all the end users.

The HEIs' end users also need to be conversant with the Higher Education and Training Laws Amendment Act 23 of 2012 (Higher Education Act 101 of 1997). This Act establishes the structures and the functions of the HEIs. Of these structures, the Council, Senate, the Principal and the Registrar each has a key role to play in the operation and the protection of IS resources used in the HEIs to protect information. Furthermore, they are important in the progress and implementation of strategies for the development of IS security e-competencies among the end users of these IS resources.

Beside the advantages of the legal environment in protecting the IS resources, the population they reach could also influence their effectiveness as the national laws would not apply to attackers living outside the country (Ciampa, 2014:150; Whitman & Mattord, 2010:442). Incidents can only act on South Africa if they involve South African citizens or permanent residents, or when outside the borders of the country, the incidents should have been committed in a South African ship or aircraft registered in South Africa or travelling to or from South Africa (Republic of South Africa, Government Gazette No. 23708, 2 August 2002).

Therefore, IS security managers and end users are required to be trained about the legal and ethical issues related to the IS resources as they emerge. This will ensure that the organisation is shielded from related liabilities. Consequently, the following section discusses the implication of IS resources and their security in the HE environment.

3.8 IS SECURITY E-COMPETENCIES DEVELOPMENT AND THE TOP MANAGEMENT AGENDA: THE ISSUE OF GOVERNANCE

As information and the IS resources that process and transmit it are important to achieve an organisation's competitive advantage (von Solms et *al*., 2011; Steenkamp, 2011; Ungureanu, 2013) and for its survival, it is important for top management at different levels to emphasise the importance of protecting the drive of active security policies that address both technological and non-technological options.

It is known that governance (risk and alignment) is about direction, control, and ensuring the success of plans from top to bottom (von Solms et *al*., 2011). Likewise, IS security e-competencies development should stem from top management directives as ICT in HEI involve administration, teaching and learning. Directing IS security e-competencies development as a top management directive can be possible through communicating security policies or related documents as part of IT governance.

Formal frameworks and institutes also support the position that top management should take responsibility for IS resources. This is evident from the aligned support to business operations and strategies by the Institute of Directors Southern Africa (2009) through the King Report III on Corporate Governance and the IT Governance Institute (2007) through the COBIT framework. Both works emphasise the focus on value delivery, alignment, and leadership through the application of best practices which are impossible to achieve if the end users are not competent in ensuring their availability and integrity.

King Report III (2009) as cited in Steenkamp (2011) suggests that the IT governance responsibility rests with the board of directors. The organisation should use the IT governance framework [with COBIT recommend – with its four domains: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME)] for compliance with its IT governance principles which ensure that ICT systems are operational and useful through confidentiality, integrity, and availability (CIA). In its recent publication, the King Report included the security of IS resources in its list of executives' responsibilities (Ungureanu, 2013).

Unfortunately, COBIT lacks details on the management of IT human resources (PO7) concerning the development of IS security e-competencies in relation to areas of focus and the levels of the security e-competencies in the HEI context, hence the need and focus of this research. As it is with any other governance issue, the development of IS security e-competencies should also be an activity in the HEI at strategic, tactical, and operational levels (von Solms et *al*., 2011 and Ungureanu, 2013). In this regard, the board of the organisation (council) should discuss its importance through their council's strategic directives, and develop a security policy for ICT security and training and development. Thereafter the policy should be implemented and applied through training and e-competencies development among the end users at operational levels.

The above position indicates that, if the top management fails to understand and communicate the importance of IS security e-competencies and their development among the end users at the strategic level, the rest of the organisation cannot

engage in such activities. There is a specific need for support from top management in providing resources for the development of IS security e-competencies, especially to translate policies to practical implementation (von Solms et *al*., 2011). If there is a failure to translate these IS resources security e-competencies at end users levels, the IT technical staff will be the only IS resources security e-competent people in the organisation.

The approach to IS resources security in the HE environment should follow the principle of Jirasek (2012) who quoted John Boyd: "*It is all about people, process, and technology*". However, people are the biggest and the most vulnerable among the three components (Okenyi & Owens, 2007) as the IS resources are made, used, and maintained by people (Hayden, 2010:272-273). In their interactions with the IS resources and related security, if people do not possess appropriate knowledge and there is no cooperation from the end users (people), these security tools could be misused or misinterpreted (van Niekerk & von Solms, 2010). As a result, they become useless for the intended purpose of protecting IS resources from misuse and threats.

Among all the security objectives that HEIs can implement to protect the IS resources, Jiresak (2012) include the following objectives: provision of security training, management of access to information, keeping IS resources resistant to malware, monitor systems for security events, manage security incidents, and monitoring security compliance, threat reporting, and implementation of security policy. Each of these objectives could have related security processes. Thus, HEIs need to develop their employees' security e-competencies to ensure that they understand, apply, and comply with the institution's security requirements.

3.9 CHAPTER SUMMARY

This chapter revealed that, as in any other business or organisation, the IS resources of the HEIs environment are just as important and core to the collection, processing, and distribution of information needed for various business decisions. The IS security e-competencies development needs to include training on the

content of IS security policy, and basic understanding of security technologies, knowledge of IS security threats and security measures, and the legal requirements.

This chapter answered the research sub-question related to the identification of threats affecting IS resources, how the researched HEIs can address the ICT threats affecting their ICT resources, and the content of ICT security e-competences training.

Because there is no single security control that can protect the IS resources and provide 100% protection of IS resources, it is important to prepare end users in both protection and actions (prevention and reaction) before, during and after an attack. This may not necessarily mean the provision of technical IS security e-competencies, but actions such as not shutting down the system to help during the investigation process.

CHAPTER FOUR: LITERATURE REVIEW – EXISTING FRAMEWORKS ON IS SECURITY E-COMPETENCY DEVELOPMENT AND THEIR CONTEXT IN HIGHER EDUCATION INSTITUTION

4.1 INTRODUCTION

To succeed in any economy or activity, organisations (including HEIs) need people, processes, and products (Holt & Perry, 2011:1). In addition to the right quantity, they need also right competencies (knowledge, knowledge, and behaviour) to deal with business activities and be productive. The focus on what people know and can do is referred to as competency-based management (Tripathi & Agrawal, 2014, and Murphy et *al*., 2012).

The adoption of a competency-based approach to work performance started long before this modern age. In their study on competency-based management, Draganidis & Mentzas (2006) trace its application from the time of Roman Empire in which the "good Roman soldiers" were selected according to their competencies.

Historically, competencies development for the workforce started in Australia after its initial introduction in the 1980s. The approach grew rapidly with an increased productivity to support the weakening economy as its overarching goal (Preston & Kenedy, 1995). This idea succeeded through a framework based on competency needed to understand, organise, and integrate the different areas of skills development, recognition and utilisation.

Besides its relation to productivity increase, the developing of employees' competencies has also a positive implication on their commitment to the organisation, improved level of job satisfaction, and motivation (Sahinidis & Bouris, 2008). All these competencies are developed to meet the current or the future job requirements.

Romani (2009) refers to the concept e-competency in his presentation on the strategies to promote the development of e-competencies as "*capability to manage tacit and explicit knowledge enhanced by the utilisation of ICT and the strategic use of information*". He continues that e-competency goes beyond the use of any

specific ICT resources. It also includes working collaboratively, to constantly innovate and create ideas while facing problems in unknown contexts.

This chapter discusses various competency development frameworks (including the Skills Framework for Information Age – SFIA, the European e-Competence Framework – e-CF, and the International Council on Systems Engineering – INCOSE competencies framework). This chapter also presents the competency classification and the methods of an effective supply of these competencies in the HEIs context.

4.2 TERMS AND DEFINITIONS

The concepts of competency (competencies) and competence (Fourie et *al*., 2013) applies to different industries and fields of studies and are translated according to the industry requirement and applied at different levels. Before proceeding into more details in this chapter, it is important to clarify what the concepts competency and competence means and how they are used in this research.

Eraut (1998) as cited in Guasch et *al*. (2010) and Chang et *al*. (2012) refer to competency as a system of complex actions including the knowledge, abilities, and attitudes required for the successful completion of tasks. Draganidis & Mentzas (2006) state that "*competency is a combination of knowledge (tacit and explicit), behaviour, and skills that give someone the potential for effectiveness in task performance*". Rodriguez et *al*. (2002) as sited in Yoon (2009a) define competency as "*a measurable pattern or knowledge, skill, abilities, behaviours, and other characteristics that an individual needs to work successfully*".

Reflecting on Holt and Perry's (2011:1) explanation, competence can be expressed in many forms by an individual. It is a reflection of his technical skills, qualifications, presentation skills, peer recognition, social skills amongst others. In other words, competence is a set of competencies (from competency), in which a competency is a single component such as knowledge, or skill (CEN, 2014b).

From the above definitions, it is clear that competency, apart from the description of its components (knowledge, skills, abilities, behaviour and attitudes); is also about practical application of knowledge and its measurement. The latter makes competency to be "*more than just the description of an activity*" or what is needed to perform an activity (Sabeil et *al*., 2011).

The difference between the two concepts (competence and competency) according to Holt & Perry (2011:2) is that competence is the ability to do something well and competency is an important skill that is needed to do a job. In other words, competence reflects a total ability of the individual while competency relates to one or many abilities that the individual holds.

Apart from the competency and competence, there is another term in use: capability. This often creates confusion and an inability to distinguish between capability and competency (Dosi et *al*., 2000 as cited by Eikebrokk & Olsen, 2007). Holt & Perry (2011:5) state that capability refers to the ability of an organisation or a unit to deliver a product or a service successfully. Ward (2004) as cited in Cragg et *al*. (2011), explains that capabilities refer to a "*firm's capacity to deploy resources, usually in combination of using processes, to affect a desired end*". This organisational capability according to Succar et *al*. (2013) comes from the interdependency between the competencies of individual employees (Cragg et *al*., 2011). In a different context, Eikebrokk & Olsen (2007) use the term capability "*as a meta-level construct referring to the strategic application of competencies*".

In the context of this research, the above discussion is important in regard to avoiding confusion between an individual's competency (technical and behaviour) in protecting IS resources and organisational capabilities in protecting IS resources. The latter (such as ICT security policy) can be, however, used to strengthen the individual's competency.

In their description on the components of competency, Bergenhenegouwen et *al*. (1996 as cited by Kim & Park, 2014) demonstrate that the structure of competency includes not only knowledge and skills in a field of study, but also innate

characteristics such as motivation, effort, enthusiasm, values, and standards. The latter all serve as motivation factors in successful performance.

Moving toward its application in the informatics field, Staggers et *al*. (2001) as sited in Ornes & Gassert (2007) relate to nursing informatics competencies as the "*integration of knowledge, skills, and attitudes in the performance of various nursing informatics activities within the prescribed levels of nursing practices*". This definition is important in the context of this research as it guides the quest for an appropriate definition of IS security e-competency.

Many authors, including Munro et *al*. (1997), Draganidis and Mentzas (2006), Mirable (1997) as sited in Yoon (2009a), and Guasch et *al*. (2010) have described the concepts of knowledge, skills, and abilities (KSAs) by using different meanings and according to a particular context Despite the different versions attached to the concepts, express the same meaning.

Moving toward e-competency, the general underlying concepts of Romani's (2009) e-competency include:

- **E-awareness**: is based on a broad understanding (knowledge-based-society, lifelong learning, usage of ICT as medium.
- **Technological literacy**: is related to confidence and critical operation of ICT acquired in formal (CDL) and informal ways (self-learning or mates).
- **Information literacy**: refers to the assessment and critical usage of information in different formats depending on the context.
- **Digital literacy**: is based on the integration of information management (creation and sharing of information) and critical thinking in multiple formats.

The following sections analyse the components of competency; particularly knowledge, skills, abilities, and behaviours as applied in IS security e-competencies.

4.2.1 Knowledge and IS security e-competencies

According to Beisse (2013:35), for a given position in an organisation there is a description of what a worker needs to know in order to do the job. This refers to a theoretical knowledge accumulated during the learning period and experience.

In their research on competence at work, Spencer & Spencer (1993) as cited in Yoon (2009a) indicate that knowledge is one of the major components of competency and it refers to "*information that one knows or it only indicates that what a person can do, but does not predict what a person can actually do*". An example relating to this study would be the knowledge of end users regarding threats to IS security.

Referring to the acquisition and state of knowledge in the field of manual therapy as Petty et *al*. (2012) present, the following can be applied in IS security e-competencies development:

- The acquisition of knowledge in security e-competencies can be gained through the indoctrination of compliance values to IS resources security. This is achieved through awareness programmes (D'Arcy, 2009 as cited by Padayachee, 2012) on technological and non-technological measures, and reporting processes on IS security related issues.
- End users of IS resources are people, and each individual is different to another in terms of the unique characteristics which they bring to the organisation (Hon, 2012; Hawkes & Weathington, 2014; Tripathi & Agrawal, 2014). Their behaviours are different among themselves and from those of automated machines which can be controlled and predicted. In this regard, end users' behaviour with regard to IS resources security becomes unpredictable and inconsistent (Vroom & Solms, 2004).

  With reference to these suggestions, the control of end users' role in the IS resources security becomes difficult and even costly to control even with the installation of security monitoring controls. Similarly, each level of employment would have its own behaviour (Vroom & Solms, 2004) and also access right to IS resources different to other levels.

- To arrive at the understanding of how end users actions' threaten the security of IS resources, it is important to assess how their knowledge, skills, and behaviour (abilities) affect the security of the accessed IS resources.

4.2.2 Skills and IS security e-competencies

Skills refer to the capacity to perform a task for a specific job (Beisse, 2013:35). An example would be the skills for troubleshooting a computer system, installing and updating antivirus software, or even scanning a storage device for security threats. Schermerhorn et *al*. (2013:13) state that skill refers to the ability of an individual to translate knowledge into action that results in a desired performance. It is a procedural or applied knowledge (De Jong & Ferguson-Hessler, 1996 as sited by Succar et *al*., 2013). As such, without skills or the ability to use knowledge, the knowledge itself becomes useless (Hayden, 2014:6).

In the field of IS security, as in other fields of study, appropriate skills (both technical and soft skills such as communication), "*is a necessary requirement to fulfil policy stipulations*" (Marcinkowski & Stanton, 2003 as cited by Padayachee, 2012). In protecting IS resources, end users can protect IS resources only if they have necessary knowledge and skills that help them understand the importance of IS resources and apply required knowledge to protect them (Padayachee, 2012), otherwise the end users cannot be interested.

4.2.3 Ability and IS security e-competencies

In the words of Beisse (2013:35), ability represents the functions that an individual either can or cannot do. An example can be the ability to keep confidential security of the organisation, undisclosed. In other words, it is part of an individual personality as the latter combines a set of psychological and emotional characteristics that reflect how a person looks, thinks, acts, and feels (Schermerhorn et *al*., 2013:29). In the interpretation Succar et *al*. (2013) present, an individual's ability to protect IS resources are part of his/her personality traits like attitudes (cognitive and rational capacity) for example analysis capacity and self-reflection (CEN, 2014b).

In this research, the word ability in relation to IS resources security e-competency is used parallel to the word attitude and behaviour which represent the end users actions in a response to a stimulus. Attitude links up knowledge and skills to achieve the outcome of an activity (CEN, 2014b).

Jones (2009) describes one of attitude (behaviour) that threatens the security of IS resources, namely the high probability of the average end user to click the CANCEL or OK button without reading the content of the message related to the button to be clicked. Furthermore, very few others could read the user license agreements or terms and condition for the software and services before they click on accept or the agree button (and include even those who continue to open unsolicited e-mails). These, and other attitudes of end users create security e-incompetency that threatens the security of IS resources that are accessed and the institution in general. As it is with e-CF (CEN, 2014b), the attitudes and appropriate behaviour in dealing with IS security are embedded in the knowledge and skills the end users possess in relation to IS resources security.

4.2.4 Behaviour and IS security e-competencies

Referring to the definition of Padayachee (2012), Information security behaviour includes a set of core information security activities that have to be adhered to by end users for the purpose of maintaining the security of IS resources as defined in the security policies. This is done to ensure the consistency, integrity, and availability of IS resources accessed by the end users whenever required.

Herath & Rao (2009) and Piccoli (2012:398) stress the importance of end users' behaviours in the protection of IS resources against security threats. This is because most internal threats to IS resources are the result of poor security behaviour of the end users. Furthermore, security awareness programmes put end users to sleep rather than improving their security behaviour (Leach, 2003).

Piccoli (2012:398) mentions a simple behaviour such as not opening an e-mail attachment from unsolicited accounts or limiting downloads from the Internet to trusted Web sites; and the ability to detect fraudulent digital certificates to go a long

way in preventing infection and keeping the IS resource protected. In this regard Herath & Rao (2009) refer to the "*appropriate use of computer and network resources and appropriate password habit*". This cannot be removed by technologies as is the case with automatic updates of antivirus and repair management.

A clear example of the role of end users' behaviour in relation to the threats to IS resources is that of a computer virus. This requires the action of end users for its spreading from one computer to another as it can only replicate on the same computer (Ciampa, 2014:79).

Leach (2003) mentions another list of threats to IS resources originating from end users' behaviours relating to omission and errors. These include the double-clicking of .exe file from an odd-looking e-mail, sharing of access password (login details) with friends, failing to backup desktop data, not logging off from your desktop when leaving the workstation, e-mailing sensitive data without proper protection, disclosing sensitive data with intention to discredit employer.

In addition to the above behaviours, Albrechtsen (2007) also recommends that users contribute to the security of ICT through actions such as locking the computer (or office) when absent from the desk, use of proper password etiquette, using e-mail, Internet, and mobile resources outside the institution's premises with caution, avoidance of unlicensed software, and the reporting of security breaches (and threats) whenever perceived in the end user environment. These are among the security e-competencies that need to be developed in end users.

As the HEIs implement security measures to prevent threats from affecting the availability of IS resources, "*unacceptable and non-malicious behaviour such as cutting of security corners to meet business deadlines should also be targeted*". This can also be done through awareness and education efforts to ensure that insiders should not plead ignorance of the rules and security policy (Sarkar, 2010 and Colwill, 2009).

To a certain degree, IS resources security has many processes, which to some extent depend on human behaviour (van Niekerk & Von Solms, 2010). Thus, the lack to equip IS resources end users with security e-competencies and them lacking positive cooperation, these processes could be misused or misrepresented. Therefore, Sarkar (2010) and van Niekerk & von Solmons (2010) recognise that threats to IS resources are a human issue or human factor. Therefore, to only deploy technology related security defense mechanisms cannot suffice in solving the problems. It is important to "combine the behavioural and organisational measures" such as security policies and training (knowledge and skills) to increase end users' security e-competencies and maximise security controls.

In general, the concept of competency appears to take many forms depending to the field and context. Eraut (1996) cited in Guasch et *al*. (2010) identify two approaches through the concept. One is related to personal skill or ability, linked to behaviour and another approach understands the concept as strategic behaviour, associated to the possibility of adjusting the performance to the context. The two approaches relate to this research given the quest for developing individual end users' IS security e-competencies and adjusting these end users' competencies levels and actions to protect the IS resources they access. In other words, these characteristics make up the personality traits that influence employees' behaviour and performance (Spencer & Spencer, 1993 cited in Chang et *al*., 2012).

Apart from the IS security specific e-competencies, it is also important to clarify that the identification of the other general and behavioural competencies as Saldaña-Ramos et *al*. (2014) and Fourie et *al*. (2013) present below, are important to consider, develop, and integrate with IS security e-competencies for a successful human capital security layer development:

- Positive attitude and motivation, judgment, and leadership;
- Self-learning capacity and ability to use IS resources;
- Ability to communicate orally and in writing in given HEI environment; and
- Organisation and planning capacity, decision taking, initiative and leadership.

To conclude this section, apart from the factors related to IS resources security spheres such as organisation, technology, and the norms created at workplace. Albrechtsen (2007) also mentions the importance of individual factors such as attitudes, knowledge, values and behaviours, as well as the motivating factor on end users' view to protect IS resources in the workplace and its general security.

The next section moves to focus on the understanding of e-competencies specific with regard to IS resources security.

4.3 INFORMATION SYSTEMS SECURITY E-COMPETENCY AND IS SECURITY

The term IS security e-competency can be described as a subset of the general IS e-competence (digital competence) which emphases the use of computer resources for leisure, education, shopping, information sharing, or any other activity for a particular purpose (Ala-Mutka, 2011 and Kreuh, 2012). In other words, it is not possible to develop IS security e-competencies without being digital competent first. For the purpose of this research, the term ICT literacy and digital literacy refers to the same concept, namely the use of computer resources to process information (Beqiri, 2010).

Lack of IS security e-competency, which involve ICT security knowledge, ICT security skills, and ICT security behaviour, has been singled out as one of the issues that organisations face in protecting IS resources that end users access to collect, process, and distribute information (Thomson et *al*., 2006). It is also important to remember that knowledge, skills, and abilities (KSA) are used as a tool for assessing candidates' ability to perform certain tasks as is the conventional standards (Kasser et *al*., 2010) in a particular field. In this case, the task is to protect the IS resources that end users access and use in HE environment.

Albrechtsen (2009) as mentioned by Rastogi & von Solms (2012) present a divide between end users and information security managers with respect to skills, knowledge, and responsibility. The main reason for this is the perception that end users lack motivation, necessary knowledge, and skills required to practice safe and

secure behaviour when using IS resources. Instead, they allow or cause adverse incidents.

In the above situation, general and security specific competencies (referred in this research as IS security e-competencies) and technologies need to be integrated and formalised in the operations of HEIs for the successful utilisation of IS resources. This is a necessity, as technological measures are ineffective to fully protect IS resources against a wide range of security threats (Faris, et *al*., 2014; Yoon & Kim, 2013).

In this research, the term IS security e-competencies was used as a combination of knowledge, skills, abilities and behaviours (attitudes) that end users need according to their job level requirement to use and protect IS resources in the HE environment. Previous sections explained in full the general meaning of competency information and defined informatics competencies as by Staggers et *al*. (2001) in Ornes & Gassert (2007) and Succar et *al*. (2013). Then, based on those work, IS security e-competency is defined in this research as:

> ***IS security e-competency is the application of knowledge, skills, and ability (behaviour) in the IS environment in order to protect IS resources against unauthorised access and inappropriate usage with intention of preserving IS integrity and availability.***

In relation to the above definition, it is important to remember that the applied knowledge, skills, and ability need to be measured against previously set criteria, standards, and learned practices in the organisational context and job levels (Succar et *al*., 2013; Abdulrazeg, 2012).

Adapting the statement of Succar et *al*. (2013) on the measurement of competency in the performance of specific activities, and based on the definition of IS security e-competency, the application of an individual's IS security e-competency can be translated into a measure of how successful the security of IS resources are maintained in the HE environment. It can be reasoned that the location of end users, their designations and IS security e-competency level could be applied as good

assessment measures for the security of IS resources that they access and for those located in their approximate environment.

4.4 IMPORTANCE OF SECURITY E-COMPETENCIES IN HEI

The HEIs and other modern business organisations rely heavily on the IS resources to supply services to their respective stakeholders. Literature reveals that much effort towards the security of ICT resources is placed on security technologies rather than on human capacity development. At the same time, the number of security incidents affecting the availability of ICT resources is internal and human related rather than technology related.

In the case above, the development of end users' IS resources security e-competencies become an important aspect of IS resources security programme in the HEI to assure the confidentiality, integrity, and availability of these resources to the rightful users. The development of security e-competencies ensures that:

- The end users consider the security of IS resources as a responsibility of all members of the institution, not only on the ICT technicians and the security technologies they use (Sedinić et *al*., 2014; Whitman & Mattord, 2010:2);
- They have to understand the spheres of IS security and how they influence the security of IS resources they access (Tshinu et *al*., 2014); and
- End users understand that the various communication technologies they use (including e-mails) carry confidential information and can be used as the channels that could compromise the confidentiality, integrity, and availability of IS resources of their respective organisations (Boshoff & van Niekerl, 2009).

The development of security e-competencies has its place in the HEI and has led to the building of proper knowledge, skills, and behaviours in the end users. It has also ensured that the end users understand the importance of IS resources and their security in the operations of HEIs.

To some extent, the security of IS resources has been pushed to the developers of IS resources (Wood, 1995). This is the case when security features like password,

antiviruses, and firewalls are incorporated with IT infrastructures. However, if end users do not have necessary competencies in using these features, they could be tempted to select an easy to guess password, mishandle the password in creating an opportunity for unauthorised users to access the information, or not setting up security features at all. The result would be the same as if the security measures were not implemented.

The following section discusses the general competency frameworks from which the IS security e-competencies framework for this research can also be derived.

4.5 GENERAL FRAMEWORKS ON COMPETENCIES

A competency framework describes a set of competencies (which are measured to demonstrate competence) that are applicable to a particular field (Holt & Perry, 2011:6). This framework is like a standard that collect best practices at different levels for the purpose of completing an activity at that particular level.
They are various frameworks that have been published for different purposes and industries. Each framework has its strengths and weaknesses:

- The generic framework level as behavioural competency framework (Orsoni & Colaco, 2013) can be adapted for any industry that needs to address behaviours, motives, traits and skills of employees in relation a specific outcome.
- The industry-specific level such as the Skills Framework for Information Age (SFIA) which focuses on the IT industry and on the technical skills rather than management skills. The other field related to this, refers to the Association for Project Management (APM) framework which measures the skills in the project management field.

For this research, only Skills Framework for Information Age (SFIA), the European e-Competence Framework (e-CF), and International Council on Systems Engineering (INCOSE) competency frameworks were discussed as they are generic and can be used to conceptualise the IS security e-competencies framework.

4.5.1 IS security e-competencies with reference to Skills Framework for Information Age (SFIA)

The development of IS security e-competencies framework requires reference to previously developed competence frameworks. One such a framework is the SFIA which is briefly discussed in this following section.

4.5.1.1 Background and levels of SFIA

The SFIA foundation owns the Skills Framework for Information Age (SFIA). Currently in its version 5, SFIA defines 96 skills (CEN, 2014c) to be fundamental to ICT profession skills which are required for the development and use of IS resources (Holt & Perry, 2011:19-23). These are grouped in six categories, each with its related subcategories and applicable levels:

1. **Strategy and architecture**: This category comprises subcategories such as information strategy, advice and guidance, and business strategy and planning.
2. **Business change**: A category including business change implementation, business change and relationship management, as well as skills management.
3. **Solution development and implementation**: This category consists of systems development, human factors, and installation and integration.
4. **Service management**: This is a category of service strategy, service design, service transition, and service operation.
5. **Procurement and management support**: A category comprising two subcategories namely the supply management and quality conformance.
6. **Client interface**: This category contains sales and marketing, and client support.

Regarding this research, the levels are too broad and abstract to explain what ordinary IS resource end users, non-ICT managers, and non-ICT professionals should do to protect the IS resources that are accessed at their levels. Also, the range of security of information between level three and level six is a little higher than what lower level end users have. Furthermore, it is apparently also reserved for employees with formal IS security education. This clarification is important because the security of IS resources is everyone's concern in any organisation. General end users should always be accommodated. Hence, for the current problem, SFIA does

not solve the challenge of end users' exclusion as has been identified in the IS security environment.

This research focuses on the description of the categories and the subcategories of the SFIA 5 framework. Therefore, summary list of the generic competencies that are applicable to each of the seven levels of the framework and their brief description can be found in version 5 of the SFIA framework (SFIA Foundation, 2011).

Holt & Perry (2011:19-23) are of opinion that generic levels are defined according to four attributes: autonomy, influence, complexity, and business skills. These are described below:

- **Level 1** – Follow: At this level the person is expected to be supervised most of the times and often seek advice. The person is also expected to possess a basic knowledge of the skill and is not expected to make significant decisions.
- **Level 2** – Assist: The person is expected to work under minor supervision and to seek advice only when necessary. The person is also expected to begin to use their judgment in making minor decisions.

  At level 2, the supervisor or manager is expected to investigate the security performance for their employees (Herath & Rao, 2009). Supervisors can conduct "from walk-in checks to monitor the workplace to evaluation logs".

- **Level 3** – Apply: A person is expected to work under general supervision and be able to make a decision as to when and where advice should be sought.
- **Level 4** – Enable: At this level a person has to work only under general direction and have a clear set of responsibilities. They can plan their work and follow the process.
- **Level 5** – Ensure and advice: At this level a person has to work under a very broad direction but will hold full responsibility in a specific area of work. The person will set their own work goals, set plans and delegate tasks.
- **Level 6** – Initiate and influence: A person has to define responsibility and accountability for a significant area of work. They are accountable for their own decisions and those of their subordinates.

- **Level 7** – Set strategy: A person has significant responsibility and authority and can be involved in defining policy and be accountable for the decisions of their subordinates.

In context of this research, it is significant that the generic competencies are basically the same for all the levels that the SFIA framework identifies with changes applied or evolution integrated as the role level changes. Sanchez & Levine (2009) state that competencies are the same across different job levels and can be identified and analysed irrespective of the organisational unit. Taking autonomy as an example, at role Level One there is need for supervision and no direction. This description changes at Level Seven at which there is need for accountability for the actions, even those of subordinates.

4.5.1.2 The SFIA framework: Not fit for end users

Beside its gaining of global popularity due to its comprehensive list of skills and roles (Asgrahani & Shankararaman, 2014), the SFIA framework is still providing for skills and roles that exist within the IT field for IT professionals and emphasises the IT skills though it is a generic framework (Orsoni & Colaco, 2013, and von Konsky et *al*., 2013). Hence, it is a difficult framework to adapt as a model for general end users' security e-competencies development. SFIA is a reference framework for the identification of skills related to the development in and for ICT resources (CEN, 2014c). The focus is to ensure that the appropriate skills of IT staff are identified, developed, maintained, and deployed throughout the organisation.

Apart from the SFIA model that can be used for assessment of IT professionals, the reviewed literature revealed the European e-Competence Framework (e-CF), which is popular among the European Union (EU) nations. This framework also helped the development of IS security e-competencies for HEIs ICT resources end users.

4.5.2 The European e-Competence Framework (e-CF)

The discussion of e-CF is based on the establishment and understanding of its background, then the discussion of its subdivision and levels of competencies.

4.5.2.1 Background and foundation of e-CF

The e-CF is currently at version 3.0 (update from version 2.0 and 1.0) as explained in the published materials of CEN (2014). It provides for 40 competencies with different levels that are relevant to the suppliers and users of ICT services. These users may be located in various departments that use ICT services such as human resource (HR), financials services, public and private business, policy makers, and the skills providers such HEIs.

The founding principle of the e-CF was to be established as a tool for creating "mutual understanding, transparency for skills required and supplied by ICT professionals at different levels of responsibilities" (CEN, 2014).

The work to develop the e-CF started in 2006 with the combination of expertise from various organisations located in Europe, including companies such as Airbus, Michelin, e-Skills UK amongst others. It was developed to be a component of EU digital agenda, for HR planning in organisations, and competence development (CEN, 2014).

The e-CF has been developed by drawing from the expertise of various industries. This gives the framework a credibility to be applied in different fields such as surveying competencies within HEI (Topchyan, 2014).

The development from CEN (2014a) as described in the previous section, demonstrates that the e-CF is not specific. This is evident from the mentioning in dimension 4 of competency A1 that a candidate must have knowledge of security (K8) and e-competence A2 related to service level management and its knowledge K6 ICT security standards. The same applies to Build area, B1 Application Development, and its knowledge K14 security in its dimension 4.

The knowledge (K6 and K14) is unspecified as there is no clarification as to what spheres of security of knowledge should be developed among the candidates. Neither is it evident from which level that knowledge should be and how that knowledge should be provided. The question on this unspecified security in e-CF

was also mentioned in Furnell & Moore (2014). These are the questions that the IS security e-competencies framework (which the object of this research) attempt to answer with a focus on the four HEIs in the Western Cape Province of South Africa.

The other critic of the e-CF is that it is applied to ICT professionals, which is a stance that excludes the other end users who have no qualification in the ICT field. It only relies on ICT resources to do their jobs. At the same time it excludes the end users from taking part or being included in the security programme of the ICT resources.

Holt & Perry (2011:120-121) explain the three INCOSE competencies framework themes as follow:

1. **Systems thinking** deals with systems engineering on high-level and generic concepts. Competencies such as systems concepts, enterprise technical environment, and supper system capability issues.

2. **Systems engineering management** deals with management aspects related to systems engineering. This includes competencies such as concurrent engineering, enterprise integration, integration of specialisms, life-cycle processes definition, and planning, monitoring, and control.

3. **Holistic life-cycle review** manages competencies related best-practice systems engineering processes. This entails competencies such as to determine and manage stakeholder requirements, system design, integration and verification, validation and transition to operation.

The competencies identified above in each of the three themes are held at the following four levels of Holt & Perry (2011:122) and Kasser et *al*. (2010):

- **Awareness**: At this level the individual will understand the basic concepts of IS security e-competencies and how these concepts fit in the HEI context of IS resources security. The individual can also ask relevant questions related to each competency. He has a theoretical understating of IS security e-competency but may not have experience.

- **Supervised practitioner**: At this level the individual has some experience of the competency and is able to demonstrate the understanding of concepts and techniques related to IS security e-competencies as part of their work.

- **Practitioner**: At this level the individual is able to guide people and lead teams' activities in the IS security e-competencies and give supervision in this area.

- **Expert**: At this level the individual is leading the competency area (IS security e-competencies as in the case of this research). They can display their experience by defining best-practice, policy or process within the HEI and the industry.

The above levels can be changed and adapted according to research requirements. In case of occupational safety and health professionals (OSHPs) Hale (1995) as cited in Chang (2012) it includes categorised levels or roles like experts, coordinators, and controllers. Draganidis & Mentzas (2006) identify the levels of proficiency for a competency as superior, average, and marginal. Gillies & Howard (2003:13-34) as cited in Succar et *al*. (2013) identify five levels (from zero to five) classified as none, basic, intermediate, advanced, and expert.

Apart from the above classification of competencies, they can also be organised in form of a curriculum (Kasser et *al*., 2010) in which the levels are the foundation, introductory, core, and specialisation. Even though they do not all relate to the IS security e-competencies requirements of end users, they can at least be useful at the first three components which can be transformed into basic, foundation, and advanced.

4.5.3.2 Critics of INCOSE competencies framework

The INCOSE competencies framework does not provide details regarding the differentiation between technical and basic, and also behaviour skills. It only suggests a list of possible skills that are of interest for particular organisations and situations (Holt & Perry, 2011:122). Apart from these critics, the framework is also believed to be lacking objectivity for the assessment of individuals' traits and cognitive skills of its intended end users (Kasser et *al*., 2012).

With reference to this research, the technical skills such as the analysis of system failure in case security attacks and the basics like reporting the security incident, and behaviour skills as not responding to unsolicited e-mail will need to be integrated in IS security e-competencies for different roles occupied by end users.

From the review of the main areas of the INCOSE competencies framework it is clear that it addresses the competencies required from the systems engineers or developers rather than the end users. However, the focus of this research falls on the systems requirements for much needed IS resources security e-competencies. The framework is applauded for being easy to use, but does not indicate if any specific skills need to be mastered by individuals at higher or lower levels.

Concerning the recommendation of a specific framework, Holt & Perry (2011:29-30) confirms that the scope of a framework and its intended audience prove to be the important factors for consideration. However, the need is for a mix of different frameworks as people will hold different competencies. Hence, this research has reviewed the two frameworks (SFIA and INCOSE) to have an overall view of the individual's total competencies requirements to be included in the IS security e-competencies framework.

4.6 DEVELOPING A FRAMEWORK FOR END USERS IS SECURITY e-COMPETENCIES DEVELOPMENT

While the three frameworks discussed in previous section focus on the general competencies for IT professionals, this research is about the development of an IS security e-competencies framework for end users (non-IT professionals). As such, while it used some of the fundamentals from the frameworks discussed, it ensures that the other components such as competencies levels and the definition of these competencies consider the levels and job profiles of end users. At the same time, the developed framework can be used to facilitate the identification, repository, and supply of the IS security e-competencies in the HEI environment. This section describes the model developed through this study by combining practices from the

reviewed frameworks, which include skills, knowledge, behaviour, and attitude that end users need to safely operate the IS resources they access.

From its definition, a competency framework (model) is described as a descriptive tool that identifies the knowledge, skills, abilities, and behaviours needed to perform a task (Kaml et *al*., 2014; Chung-Herrera et *al*., 2003 as cited in Gayeski et *al*., 2007). From the perspective of its role, the framework acts as an intermediation tool between competencies, role performance and job satisfaction (Madter et *al*., 2012). In light of this research, the framework described the knowledge, skills, abilities, and behaviours that end users need to protect the IS resources and serves as a tool for the development of these IT security e-competencies in the HEI environment.

Once the ICT security framework has been developed, it can serve as a tool for the analysis of the IS security e-competencies to be included in situations such as the creation and updating of job descriptions, training and development on IS security, recruitment and the selection of potential employees for certain positions (Gayeski et *al*., 2007) and the development of an overall security plan for HEIs.

To arrive at the development of such a competency framework, certain important constructs (steps and principles) of the framework such as those of Draganidis & Mentzas (2006) and Holt & Perry (2011:103-121) need to be considered and included in the model to ensure that it is aligned to mutual principles. For the purpose of this research, the steps are divided in two phases:

- **Phase 1** is related to the identification of the steps and components needed to be included in the competency framework and is presented in this chapter.
- **Phase 2** is related to the development of the actual IS security e-competency framework after the analysis of collected data and explored in Chapter 8. This phase is important as HEIs' security e-competencies framework should relate to the specific practices of its environment and should support the culture as well as integrate the particular work and end users' requirements (Saldaña-Ramos et *al*., 2014).

Apart from the above-summarised steps, Holt & Perry (2011:103-121) provide also the following phases and their related steps that need to be considered when developing a competency framework and other necessary components:

Phase 1: Steps and components of competency framework: The phase comprises the following steps:

- **Step 1** – Identification of the reason (purpose) for the competency framework is to be developed. The step is common to any other project and any other work to be undertaken. In the case of this research, the reason is to understand and describe the IS security e-competencies among the different levels of end users in the HEI. It furthermore needs to explore how these security e-competencies can be supplied to end users to ensure maximum participation.

- **Step 2** – Generation of relevant stakeholders' profile. A relevant step as it helps to identity the different roles the end users portray. For the purpose of this research, every employee is considered to be the end user of IS resources. These end users are then separated by the activities they are performing with reference to their roles on IS resources.

- **Step 3** – Identification of the sources framework. The design of the company's specific competency framework should be in line with the best practices standards established. Because one framework can be insufficient to cover all the competencies required, there is a need to combine two or more frameworks. In the case of this research, the INCOSE framework and SFIA have been combined as a frame of reference. These frameworks were used to create a structure that could accommodate the competencies identified in the literature and in-depth interviews with representatives from four HEIs.

- **Step 4** – Identification of relevant competencies. The competencies identified in the source frameworks such as SFIA were at high level and appropriate for IT professionals. They needed to be adapted to the HEIs' own environment and the purpose of the framework.

- **Step 5** – Setting the competency levels. For each competency there is a level that applies to the end users' roles with reference to the framework purpose. In addition to the competencies level, the indicators for each level also need to be set as they are the basis of competencies assessment.

  Armed with these five steps and identified components, the next step was to generate the IS security e-competency framework for the HEI environment, which is in line with improving human capital (HC) Saldaña-Ramos et *al*. (2014).

Phase 2: The phase manages the development of the actual IS security e-competency development framework. It uses the data that is collected from the literature review and interviews with participants through this research to develop the actual framework that is presented in Chapter Eight of this research.

The steps provided above are also summarised in Draganidis & Mentzas (2006) for activities associated with key processes for management when competencies were identified. The following four sequences are described:

- First, competence map (model or framework) and the required levels for each role need to be obtained. This is important as the level of competence for assistant work is different to that of a supervisor and level of challenge differs according to the role level as well (Baartman & de Bruijn, 2011).
- Second, carry out the gap analysis of employees competencies. This is to assess if the current level match the required level of competencies for the specific role level.
- Third, develop the competences based on the gap identified from the analysis result per role of employees.
- Fourth, monitor the progress continuously. This stage is important in the case of IS security e-competencies development as there is continuous monitoring of competencies due to changes in the environment.

Apart from the above steps, Armstrong & Taylor (2014:91) also suggest useful steps for developing a competency framework which are presented in Appendix B.

After the description of the two model frameworks and identification of the steps for developing the final framework for this research, the following section review some of the research that were conducted in competencies development in other IS sub-fields and the other industries to share in their experience.

4.7 PREVIOUS RESEARCHES ON IS COMPETENCIES

As the reviewed IS relevant literature did not reveal any work on security e-competences, this study had to rely on the literature from other fields to serve as a guiding material to build the IS security e-competencies framework of this study.

4.7.1 Competencies in other industries

The multidisciplinary nature of IS means that some concepts and theories are borrowed from fields such as psychology, sociology, and pedagogy to be integrated into IS (Karjaleinen & Siponen, 2011). This fact has directed this study towards exploring the development of competences in other industries that might be relevant to the development of IS security e-competencies in HEIs.

For example, the investigation of the competencies for the airline cabin crew members in Korean airline by Park & Kim (2014) revealed that the development of competencies among the employees has an impact on the improved image of employees and the organisation. Authors identified eight main competencies: appearance and attitudes, physical fitness, customer-oriented skills and company loyalty, knowledge of foreign cultures and languages, emotional intelligence, skills for inflight services, past work experience, and interpersonal skills. Linked to this research, it is important to emphasize existence of knowledge, skills and the personality-based competencies that can be linked to attitude and behaviour.

Suh et *al*. (2012) classify the necessary competencies for managers in the hospitality industry in six dimensions: (i) Interpersonal skills (ii) supervisory skills, (iii) hospitality skills, (iv) leadership skills, (v) communication skills and (vi) food and beverage management skills. Suh et *al*. (2012) demonstrate in their study, as this research also show, that the competencies in the hospitality industry as well as in IS security

include both field knowledge and non-field related knowledge. The communication skills are also important as it will enable IS end users to appropriately report possible security threats.

4.7.2 Competencies in other IS related fields

In general, the study of competencies in the IS field is not a new undertaking as it gained more attention and management focus in this modern information age with the proliferation of computer systems. However the focus thus far was on IS security professionals rather than on end users - as demonstrated in the three frameworks presented previously.

In the study on end users' computing competency in which 338 respondents from various industries were surveyed in South Korea by Yoon (2009a), three IS security e-competencies were identified among 17-item instruments that measure the end user competency in relation to IS security. These three IS security e-competencies are (i) end user ability to establish and manage the security of computing systems, (ii) knowledge related to computing security, and (iii) the recognition of end user computing security.

In another research which focused on computing competency of end users and their task performance, Yoon (2009b) concluded that "*individual's computing capability has an effect on his performance of a given tasks in a business environment that depend on computing*". The factors that have a direct influence on their performance include the knowledge of computing technology and computing utilisation ability. From Yoon's (2009) logic, this research also believes that the IS security e-competencies contribute to the improvement of end users' abilities to protect ICT resources and organisation's performance.

With reference to this study, these findings are important in the sense that they show that IS security e-competency of any kind is important not only for IS security experts, but also for anyone who access the IS resources for the performance of daily activities.

In the early stage of competency research in the Library Information Science (LIS), Gorman & Corbitt (2002) identify four core competencies which were subdivided in four areas that incorporate basic knowledge for library science professionals: (i) client needs and services, (ii) management of people and resources, (iii) technology utilisation, and (iv) organisation of knowledge. Among the competencies identified that could be adapted into IS security at different levels, the following are included:

- Demonstration of understanding of information seeking behaviour and appropriate responses.
- Demonstration of knowledge of information sources.
- Evaluation of the quality and appropriateness of information.
- Leading effective strategic and operational planning, evaluation, and marketing processes.
- Developing and implementing essential information policies and procedures. And
- Application of different learning theories and methodologies.

4.8 DEVELOPING IS SECURITY E-COMPETENCIES IN HIGHER EDUCATION

Developing employees' IS security e-competencies could not be of much importance in the old age when ICT infrastructure environment was considered as ivory tower which was accessed only by experts and well identified employees. In the current knowledge-based economy, the reliance on ICT resources, their pervasiveness, and dissemination of information and key applications such as ITS and MAS (in the case of HEI), the rendering of the development of IS security e-competencies is a necessity.

In fact, the nature of knowledge-economy (Knights & Willmott, 2012:199) and the reliance of HEIs on the integrated ICT systems using the global platform, these systems become vulnerable to security breaches internally and externally. Thus, the systems require the end users to be vigilant at all levels (IJHC, 2007), but also to rise to the challenges that the security threats present.

Therefore, training end users and developing needed security e-competencies for the protection of IS resources becomes an important task for HEIs in helping its

employees to be aware of the value of IS resources (including information), increase the level of awareness on IS threats, and also become aware of what goes in their trash (Okenyi & owens, 2007). This apply to all employees who deal with IS resources in addition to their formal qualifications and their daily job activities.

4.8.1 Training, awareness programme, and education

For the purpose of IS security e-competencies development, it is important at this stage to be reminded that training and awareness are different initiatives. According to Robinson (2006), the awareness strategy targets the broader range of people as all of them cannot attend the training. The goal of awareness is to make people understand the value of the IS resources they use in order to protect them. The awareness campaign according to Eminağaoğlu et *al*. (2009) is added to training courses to complement the training as employees can forget the content they were exposed to during the training.

In addition, the awareness materials can be distributed in the form of posters, brochures, animated movies, animated electronic messages, online quizzes with prizes (Eminağaoğlu et *al*., 2009). All these materials must be designed by relevant experts to make them user-friendly and attractive to employees and must be short, interesting, and enjoyable movies (Eminağaoğlu et *al*., 2009).

To be specific, Whitman & Mattord (2010:191,198-199) differentiate between awareness, training, and education with regard to ICT security in the following way:

- **Training** is intended to build knowledge for skills development on an intermediate timeframe. The methods for developing the skills include practical instruction lectures, case study workshops, and hand-on practice.
- **Awareness** programmes are intended to focus on short-term provision of information that end users need to recognise the importance of ICT security. The methods mentioned for building competency in this regard include newsletters, posters, and media videos. It also set the stage for security training by instilling the importance of ICT security among end users and changing their behaviour in handling information and other resources.

- **Education** is intended to foster insight and understanding for the long-term. The methods recommended include theoretical instruction discussion seminars, and background reading on the information security.

In their research on improving end users' behaviour and awareness on IS resources security, Lund & Aarø (2004) suggest that "*programmes combining different kinds of measures have the most positive effect' as opposed to the training methods only*". Measures to include in this regard, are IS resources security campaigns, education, and rewards. However, these options can be extended to other methods.

Whichever method is used to deliver training to end users on security e-competency in the HEI environment, the channel used to convey the message and the level of the message conveyed need to be in par with the level of the target participants to ensure maximum participation and effectiveness. The message should also be accessible for the targeted participant.

4.8.2 Training and awareness programme costs and benefits

The implementation of the IS security e-competencies development programme can be a costly exercise for the HEIs in different ways:

- At one hand, it is related to the operation of the training, participation, and the availability of ICT security expertise.
- At the other hand, the change in ICT threats and innovation in the ICT industry causes training to become more complex. The need to continuously adjust the security e-competencies of end users become more permanent for as long as the HEIs continue to rely on IS resources to manage the operations of HEIs and any other organisation.

In reality, the costs for IS security e-competencies development programme can be both direct and indirect. The direct costs include those related to training materials and salaries for trainers, while indirect cost include the lost time spent advocating for security and attending security training by employees (Johnson, 2006).

Among the benefits derived from the training and awareness programme include the specific advantages of Johnson (2006): (i) increased confidence from stakeholders (business partners, customers, and suppliers) when dealing with the organisation, (ii) reliability of information processed by end users, (iii) decreased number of internal incidents and errors as a result of proper use of resources, (iv) better and earlier detection of security incidents, (v) improved compliance to the law and internal requirements, and also (vi) improved productivity and employees' moral.

Apart from technical support to ICT security, training and awareness influence (benefits) the security of IS resources. Whitman & Mattord (2010:189) mention the following influences: (i) Improving the employees' behaviour on ICT security; (ii) Informing end users on how to report the violation against ICT policy; and (iii) Ensure that employees are held accountable for their actions.

Despite its benefits to the organisation, to be effective security training and awareness programmes, senior executives need to enforce it through their security policy (Henry, 2004 as cited in Thomson & von Solms, 2006) or even their behaviour modelled according to the security culture.

Even though training on IS security is an important aspect for HEIs, it is important to note that it adds more challenges to the existing responsibilities of end users. Quoting Reissmueller, Lynn (2009) confirms that end users are primarily responsible for the job they are paid to do and not for IS security. According to the author, end users cannot be expected to be security experts, but they can be taught to notice when something goes wrong and who to call when a security related issue arises.

This is in opposition to the training that is conducted in other organisations such as the U.S. military services and the Department of Defense (DOD) agencies. These institutions' training goal is to create a "cadre of information assurance professionals in technical and management position in line with their warfare strategy" (Robinson, 2006). Security awareness must be on-going "to keep knowledge fresh and real" (Lynn, 2009) with the implementation of approaches such as ICT security week, regular alerts, and weekly e-mail reminders (Robinson, 2006).

The following section reviews two models (Kim and Park model and the triple A (triple action – Acquire, Apply, and assess) competency model as training model) of competency training that can be adopted or adapted for the training and development of end users' IS security e-competencies in the HEI environment.

4.8.3 Kim and Park model for competency-based training

Apart from its promise to improve the image and output of the organisation and the individual employees, the competency-based training is important as it emphasises on closing the gap on necessary competencies in performing tasks rather than providing skills and knowledge that have no immediate impact on the performance of tasks. In this context, the training can meet the requirements of developing the needed skills to achieve organisational goals (Sahinidis & Bouris, 2008).

With reference to competency-based training and learning, Succar et *al*. (2013) clarify that the learning is based on the previously identified specific competency items (or outcomes) which are embedded into a learning module for a specific audience. In this regard, training becomes focused and provides end users with needed skills on IS resources security rather than broad and unnecessary knowledge that is not required at their level of employment, which enforces the retention of and application of gained skills in the business operation. Referring to Sahinidis & Bouris (2008), the larger the gap between employees' required knowledge, skills, and attitude needed in security e-competencies, the higher the level of exposition of organisational IS resources to the possibility of being compromised as the employees are unable to identify the threats or perform appropriate actions in mitigating heir effects.

From the literature reviewed on competencies development, no model was found that could be used for IS security e-competencies analysis and development in HEI apart from the competency-based model found in the simulation of the competencies for the airline cabin crew members in Korean airline industry by Kim & Park (2014). This model is presented in Figure 4.1 in which the authors identified the steps to be taken when designing competency-based training.

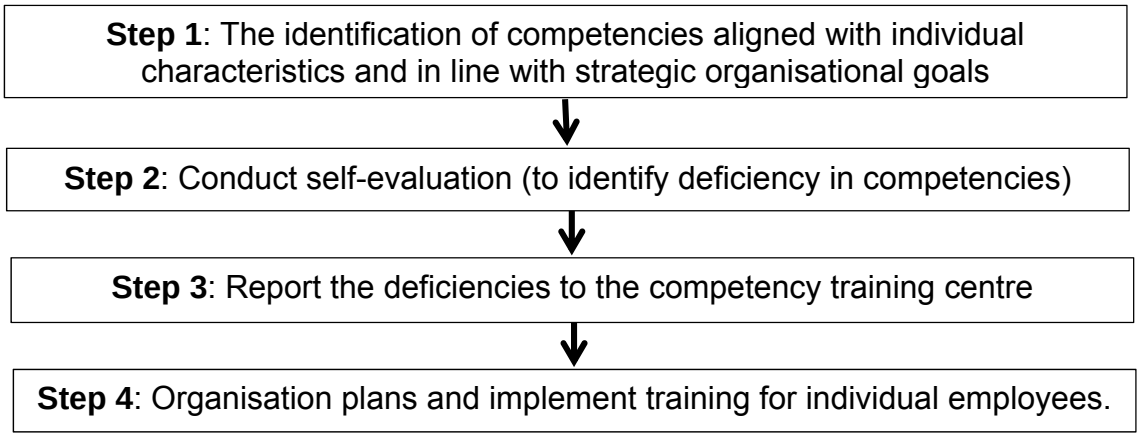


Figure 4.1: Competency-based training steps

(Source**:** Adapted from Kim & Park, 2014)

In relation to Figure 4.1, the identification of competencies alone in the tourism industry, in the ICT security, or any other field is not a guarantee for determining the training or educational criteria. It however helps in the process of identifying the needed knowledge, skills, and attitudes required (in the case of this research) for identification. It also assists in fighting security threats to IS resources that originate from the employees e-incompetency. In this context, IS security e-competencies that end users require can be delivered according to their level and role in their respective HEIs.

The consideration on levels and roles of employees is important and has also been emphasised by Morelock (2012) and Sedinić et *al*. (2014) when they mention the need for tailoring the training in accordance to the skills levels of employees. This includes the presentation of technical training using technical terms to technical people and non-technical training for non-technical end users with consideration of their job level. In addition, each level of employment requires a unique set of skills and personalities. If this requirement is not managed, it creates a challenge in maintaining interest and engagement of participants when the materials are not related to their responsibilities or level (Moreleck, 2012).

4.8.3.1 Ways to identify competencies in an organisation

With reference to the Kim and Park model provided in the previous section, the identification of competencies phase is important and worth analysing further as it serves to set-off the rest of the process.

There are various ways to identify employees' competencies levels (IS security e-competencies) in an organisation. Succar et *al*. (2013) suggest the following:

- The analysis of job advertisement descriptions as the organisation created;
- Revision of academic literature and industry publications on ICT security;
- The harvesting of competency requirements from information security associations and experts through data collection techniques such as interviews, focus groups and surveys; and
- The adoption and adaptation of skills inventories and competency pools similar to those suggest by international bodies and standards such as SFIA and INCOSE referred in this research.

4.8.4 The triple A competency model as training model

Another model that can be adopted and adapted to provide IS security e-competencies to end users in HEI is the triple A competency model of Succar et *al*. (2013). The model identifies three complementary actions on the outer circle that may help in the process of gaining and applying IS security competencies. These are:

- **Acquire**: The acquisition process refers to the learning activity that takes place during the training, workshop, or any other learning method applied for this purpose that suit the competency requirement. This can be practical learning in the computer laboratory setting or in the class setting. To keep employees engaged during the training delivery period, Morelock (2012) advises that employees should lead sessions and share their practices and their experiences.

- **Apply**: This process includes the activities related to using the learned competencies to produce a specific outcome. Two of the three approaches suggested for the application of competencies include:

- Population of a task list for the initiation of process – this approach refers to setting a step-by-step guide for completing a task or creating a quality check list. In the case of this research, it can be the listing of steps in dealing with online security threats or sensitive documents.
- The generation of a standardised mind map or flow chart diagram for testing or dealing with ICT security threats.

- **Assess**: Assessment ensures that employees' IS security e-competencies (knowledge, skills, and ability) in dealing with IS security threats are developed and are in line with previously set standards for particular levels and roles in the organisation. This is in line with the purpose of externalising implicit knowledge with a purpose of identifying a gap for training and assessing the organisation performance in terms of the current IS security e-competencies.

Apart from the outer circle, the model (triple A competency model) also identifies an inner circle which is useful and can be adapted in the competency-based training. The inner circles include the following adapted three elements:

- **Identification of what should be acquired**: This refers to its focus on the competency-based training, the needed indicators of competency category to be identified and included in the training modules in such a way to address the training needs of the specific level and role of employees.
- **Learn what was identified and what will be assessed**: This refers to the use of specific, identified training methods and the method for assessing learned skills.
- **Apply, monitor, and certify what has been applied**: As the threats to IS resources are dynamic, the organisation should also ensure that it continuously monitors the learning curve to ensure that the employees apply current IS security e-competencies.

After its description, the triple A competency model is adapted from Succar et *al*. (2013) and presented in Figure 4.2.

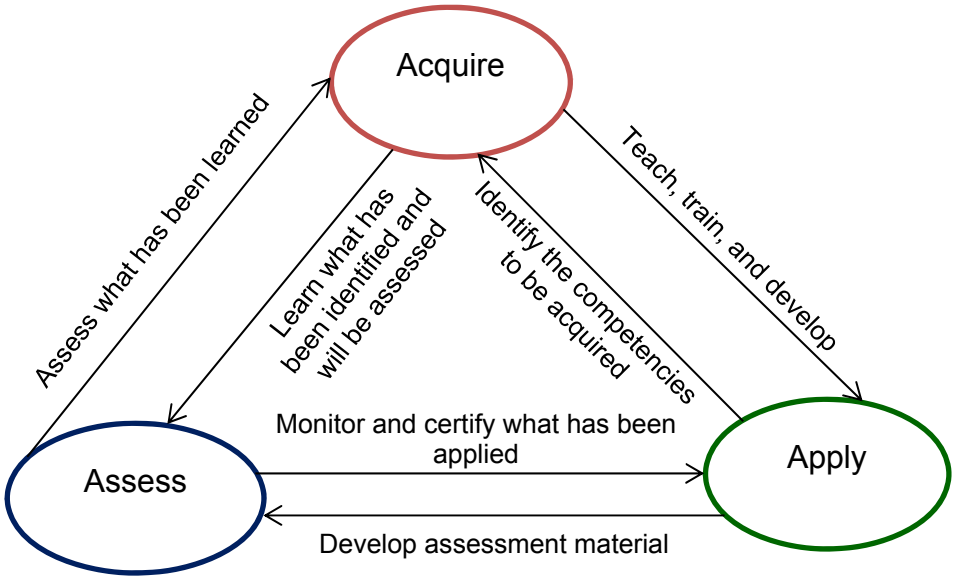


Figure 4.2: The triple A Competency model

(**Source:** Adapted from Succar et *al*., 2013)

The competency-based assessment, which Wilkinson (2004) refers to as a testing process, is different to other forms of testing (such as knowledge-based or classroom conceptual mode). In the case of this research, it is complex and broadly applied as opposed to theoretical knowledge acquired in a formal classroom context. Beside its broad application, the competency assessment is also contextualised to the workplace challenges and cases (Heather, 2004).

4.8.5 Training and development from IS and security related fields

Training and awareness for IS resources security is an important part for better security standing in any organisation. It is also required for the improvement of end users' behaviour and awareness in handling the IS resources (Albrechtsen & Hovden, 2010). Zafar (2013) classified the training of end users on IS security, along with other factors such as security policies and legislation and regulation to be among the contributors towards the security of HRIS and e-HR security.

Williams (2012) stresses the importance of a holistic approach to IS security given the rise of security threats and increase in ingenuity of attackers (black hats). To

train for the holistic approach, the author suggests the practicing of various defensive techniques starting with security policies, security audits to identify security breaches and other problems (Williams, 2012).

It is also important to move away from the current training and awareness that "emphasises only on the vulnerability related to the various information security threats and what should be done to reduce such vulnerability" (Rezgui & Marks, 2009). It is essential to now include awareness of the existing "means to controls the information security threats" (Rhee et *al*., 2009). The latter training and awareness refers indirectly to both security technologies and non-technologies controls to be added to the identified security vulnerability threats.

To ensure that employees participate in the awareness and training campaign, Robinson (2006) mentions that at Interior, IS resources end users are required to pass a mandatory online exam each year. If the employees do not take the test by a certain date, their access to computers and Internet can be cut off. In the same research, the author suggested that another U.S. department (namely USAID) which has received good scoring on information security, uses a daily test for all its employees from the highest to the lowest office before they access the IS resources.

Another important study on IS security training was conducted by Keith et *al*. (2007) From the importance of training and awareness campaigns for ICT security, Jones (2010) suggests that "one approach that might improve the end users approach to information security is by making security processes open to them". This can only be possible by the introduction of training and an awareness campaign. The training and development, and the awareness campaigns are the best ways to improve this users approach to ICT security.

In fact, Eminağaoğlu et *al*. (2009) quoted Tipton & Krause (2007) and IT Governance Institute (2008) who advocate the importance of people in an organisation as the primary and most critical line of defence in the protection of IS resources. This is besides the existence of security counter-measures and technology solutions in

dealing with security threats. “They are neither correctly nor effectively deployed” or they are sometimes outdated to stand against new and evolving security threats.

The above findings explains only the reasons for security technologies not being able to deal with all the threats to IS resources and the training of employees in security related aspects that match the weaknesses of security technologies. Eminağaoğlu et *al*. (2009) continue to say that not only technical security training of IT staff needs to be improved, but also information security awareness and training have become a must for everyone. This is because the successful implementation of security controls and measures depends on the level of training and awareness of end users (D’Arcy & Greene, 2014; Shahri et *al*., 2013) which are emphasised in the IT security policy. The employees are also to be well informed (trained) on this security policy.

As Padayachee (2012) and Albrechtsen (2007) mention, incompetence (unskilled employees in security e-competencies) may result in individuals failing to recognise the value of security measures or even overlook the security measures if it hinders them from completing their tasks. Colwill (2009) refers to people’s (end users) failures to report the wrong activities due to their misunderstanding of its significance, or failure to recognise that it was their responsibility to report, or that they just even do not know how to report the incident.

The importance of training in the protection of IS resources was demonstrated by CPNI (2009) as cited by Colwill (2009). The report suggests that training should be listed with the security methods (non-technical measure) to be implemented among the end users.

Apart from the focus on detecting attacks, IS resources security training can be extended to a much larger aspects of information security. This could include the identification of threatening e-mails, reporting of malicious activities, access control and password, safe internet surfing habits, protection of movable assets, the use of shredder to dispose document containing valuable information, and technological controls.

In the study on universities' security policies, Doherty et *al*. (2009) discovers that security training for end users has been given prominent coverage in many security policies that were accessed. This campaign for training shows to uphold the non-technological aspect of IS resources security is gaining momentum across the world. Hence, this research investigates it application by the universities in the Western Cape.

As employees' behaviours change (Rhee et *al*., 2009) and the security threats also change, the security and awareness training for end users should also be a continuous activity in the calendar and operations of HEIs with possible changes as long as the HEI has introduced the training. This is also relevant and true for any organisation that relies on IS resources to collect, store, process and transmit information.

These findings present best way to transforming end users from the weakest link and vulnerability state in IT resources security (Yildirim et *al*., 2011; Agrawal & Khan, 2014; Banga et *al*., 2014) to the strong link and first security layer in defence against IT resources security threats. This is in reference to their ability to understand and stand against the accidental and non-accidental security threats from internal or external environment (Rhee et *al*., 2009; Thomson & von Solms, 2006; Vroom & Solmons, 2004). This double role of employees in the IS resources security make them act as the defence line against security threats at one hand, but on the other hand, the weakest link if not provided with effective security competencies to protect IS resources.

Finally, Humphreys (2008) states that IS security awareness is part of good business practice. Education, training, and awareness form part of organisational education programme intended to reduce security breaches as a result of employees' ignorance and lack of awareness (Zafar, 2013). Among the three, training and education should precede the awareness as employees need to know about the security and threats in order for the awareness to be effective later (Sedinić et *al*., 2014).

As such, all insiders need to be made aware and trained (from the induction or orientation day and continuously during the employment) on the risks affecting IS resources and related procedures for dealing with security risks so that they can conduct their operations in a secure environment (Smith, 2004). Hence, developing end users' security e-competencies in protecting information resources is of the same importance as implementing the security control mechanisms.

4.9 CHAPTER SUMMARY

This chapter explored the competency frameworks and concepts related to IS security e-competencies development. It also investigated how the frameworks in this research can be used to create an appropriate framework for security e-competencies supply in the HEI environment. In this review, the chapter answered the sub-question on the importance of IS security e-competencies, and their development.

In order to ensure that the required information systems security e-competencies are identified and developed among the end users at different levels of employment in the organisation, there is a need for the organisation to establish a guiding framework (IS security e-competencies development framework). This guiding framework is for a formal supply of IS security e-competency to end users that can be used to match employees' security e-competencies and their classification level in the HEIs environment.

End users are not able to protect the IS resources through the mere application of a guiding framework. Thus they need to have the IS security e-competencies in the identified spheres of IS security which are appropriate and applicable to their job level. These were all identified in this chapter and specifically applied to the four HEIs that participated in this research. The competencies frameworks reviewed could not provide an answer to the needs of end users' IS security e-competencies due to their focus on the ICT security professionals. Hence, this chapter continued to identify and discuss best approaches that can be adapted for the supply of IS security e-competencies in the HEI environment.

Chapter 5 discusses the research methodology and methods applied in this research that arranges the research, collect and analyse the data.

CHAPTER FIVE: RESEARCH DESIGN AND METHODOLOGY

5.1 INTRODUCTION

This chapter discusses the research design and methodology, which includes a philosophical foundation that underpins a functional-interpretive approach to this study. It also reflects on the approaches and application of research methodology, the methods used for data collection and analysis.

Generally, this study used a case study methodology as it is seen as a viable and valid research strategy (Klein & Myers, 1999) since the researcher studied the information systems topic in its natural environment. This allowed for a generation of the IS e-security competence theory from practice (Dooley, 2002). His methodology also assisted in understanding the nature and complexities of the processes for securing organisational ICT security resources (Gable, 1994).

Using a multiple case study strategy, the interviews, questionnaire, and review of previously published data were applied as instruments of data collection. This research used a mixed research method approach that guided the sampling strategy. Content Analysis (CA) and Grounded Theory (GT) approach of data analysis were used for the analysis of qualitative data and descriptive statistics techniques were used for the analysis of quantitative data.

5.2 RESEARCH DESIGN

The research design generally represents research steps from the conceptualisation phase, data collection and analysis in order to develop an appropriate framework, conceptual model or theory. In other words, the research design represents *"a blue-print or a detailed plan for how a research study is to be conducted" (De Vos & Fouche, 1998:123)*. Research design, in that regard, has a role of ensuring that *"the evidence obtained enables the researcher to answer the initial question as unambiguously as possible"* (De Vaus, 2001:9). Hence, the research design in this study was particularly useful as a guideline for data to collection and analysis (McCaston, 2005) as it was considered as the plan that connects the conceptual research problem and empirical research (Van Wyk, 2012).

Following these guidelines and De Vaus' (2001) advice that the design should not stem from the basis of how to carry out the plan but rather why, the research design of this study included the following:

1. Identification of the research problem.
2. Establishing the research questions and objectives.
3. Establishment of preliminary interviews with experts to determine the relevance of the research problem.
4. Undertaking the review of the pertinent literature.
5. Conceptualising the literature findings in order to develop a framework for empirical testing.
6. Studying and selecting the appropriate research methodology.
7. Conducting empirical data collection and the analysis of the collected data.
8. Discussing findings.
9. Proposing the final framework for addressing the identified research problem..

The selected research design helped in highlighting the purpose of this study through the Maxwell's *Interactive Model of Research Design* which involves the following (Maxwell, 2008):

- *Goals*, including probing the merit of the study, the issues to be clarified, and the significance of the study;
- *A conceptual model*, which inter alia guided the definition of the scope of this study;
- *Research questions*, as a part of the research design process that ensured that the data sources, data collection and data analysis would lead to the relevant and valid results;
- *Methods* to assist in the identifying of appropriate techniques to collect and analyse data as well as to understand the integrating of a mixed method approach as applied in this study.
- *Validity*, to verify both the quantitative and qualitative results of this study.

As the research design typically focuses on the type of study and results expected, the research methodology, which is described in the following sections, focuses on the actual research process, the type of tools and the procedures to be used (van

Wyk, 2012). The selection of research methodology and determining the appropriate methods for this study originated from considering different philosophical perspectives and research paradigms. This was applied through following this research stance and particular description of used methods and techniques.

5.3 PHILOSOPHICAL APPROACH OF THIS RESEARCH

This section discusses the application of philosophical approaches in terms of the different viewpoints and way of interpretations. It can also be discovered through concluding on research phenomena such as the development of IS security e-competencies in the HEI environment.

5.3.1 Philosophical perspectives

In all its forms (qualitative or quantitative), social research is based on specific assumptions regarding the make-up of valid research (Avison & Pries-Heje, 2005:241). The research assumption that is used to describe the research approach is known as the epistemological stance. This is the science of knowing or making assumptions about knowledge and how it can be obtained (Babbie, 2008:6; Myers, 1997).

With reference to the philosophical perspectives, the underlying epistemology distinguishes four paradigms: positivism, post-positivism, critical theory, and constructivism (Guba & Lincoln, 1998; Myers, 1997; Shkedi, 2005:18; Denzin & Lincoln, 1994:109; Punch, 2014:16). On the other hand, Henn et *al*. (2006:10-13) and Gray (2014:19-24) maintain that there are only two groups of paradigms that influence how research can be conducted, data collected, interpreted, and results published. These groups are positivist and interpretive, with the former associated with quantitative research strategies and the latter with qualitative research strategies.

The positivist paradigm considers the existence of the research world as independent (and external) of the knowledge of this world (Gray, 2014:19-21). In regard to this research the properties of this world, such as those of IS resources security e-competencies development, can be observed and measured as facts

(Henn et *al*., 2009:219; Gray, 2014:19-21). This is also applicable to IS security e-competencies from the end users' habits, knowledge, and skills perspective. Some examples include the opening unwanted e-mails, downloading items and/or files from any website, leaving critical applications and IS recourses open and unattended to be observed or their results such as spreading of viruses can be observed in a real environment. The positive paradigm, considering cause and effects (Henn et *al*., 2009:14), was used to explain the effectiveness (existence or non-existence) of the social phenomenon (IS security e-competencies development) and relationships to IS resources security.

The above aspects of the positivist paradigm lead to implications such as the use of structured research design, reliable methods, and the generation of large-scale statistical-based studies (Kumar, 2011:11-13, Henn et *al*., 2009:11-15). All these are the requirements of quantitative research (Hennink et *al*., 2011:16, Kumar, 2011:20 and Henn et *al*., 2009:14).

The interpretive paradigm, on the other hand, derives from the cultural interpretation of the social context and the viewpoints of people living in the environment rather than cause and effect (Henn et *al*., 2009:14; Gray, 2014:23). This is because people respond actively to the conditions in their environment. This paradigm considers that "reality is socially constructed" (Hennink et *al*., 2011:15), given people's experience and history in the particular social environment such as HEI.

In the context of this research, the understanding of the IS security e-competencies in one HEI may be different to the other HEI or other business sector. The reason for this is the historical and cultural interpretation of IS resources security in the HEI on the basis of how end users' behaviour were shaped by their environment. Thus, the interpretive paradigm, suits the unstructured and qualitative research for data collection methods such as interviews (hear) and observations (see). These methods are considered as valid for building theory from research and generally starts with research questions, and generation of small scale but intensive data (Hennink et *al*., 2011:9-16,132; Kumar, 2011:11-13,20; Henn et *al*., 2009:11-15).

Next, the confusion of linking qualitative research to interpretive paradigm merely on its foundation of understanding and explanation of the social phenomenon is removed. In the same instance, the positivist paradigm to be linked to quantitative research only on the stated grounds of Blanche et *al*. (2006:7) and Henn et *al*. (2009:15-16) has been challenged by some researchers (e.g. Avison & Pries-Heje, 2005:226; Myers, 1997). These researchers claim that qualitative research may adopt any of the four paradigms (positivism, interpretive, critical theory, post-positivism, and constructivism), depending on the philosophical assumption of the researcher. Gilbert (2008:138) supports the same view by maintaining that mapping one paradigm to a specific method is pure caricature, even though the distinction exists.

Generally, qualitative and quantitative methods draw on different paradigms (Gilbert, 2008:137). However, a case study research, one of the qualitative methods, can be positivist (Yin, 2002) or interpretive (Walsham, 1993), or critical (Myers, 1997). In the context of this research, due to its diverse characteristics, the type of problems addressed, disciplines, and strategies used to collect and analyse data (Ramesh & Glass, 2002), the IS field presents endless possibilities of adopting diverse research paradigms to investigate related knowledge.

Other authors who have investigated the nature of knowledge in social science such as Burrell & Morgan (1979:21-24) describe four paradigms which are linked to two extremes. At one extreme are those that are more supportive of the positivist theory such as the functionalist and radical structuralism and those that are supportive of anti-positivist theory such as interpretive and radical humanist. Other researchers in the field of information systems refer to research paradigms (positivist and interpretive) as research approach (Ramesh & Glass, 2002).

5.3.2 Research paradigms described

This section describes a particular research paradigm and the way they influence the understanding of IS security e-competencies development and supply in the context of HEI. For the purpose of this research, only the functionalist (positivist) and interpretive (anti-positivist) research paradigms of Burrell & Morgan's (1979:22)

classification are discussed. Specific reference to their contribution to this research is relevant to the theoretical foundation as represented through the Activity Theory (AT).

These paradigms (functionalist and interpretive) are the dominant paradigms used to conduct research in the field of information systems (Gray, 2014:37; Ramesh & Glass, 2002; Avison & Pries-Heje, 2005:221-224; Myers, 1997). The interpretive paradigm, in particular, fits the participants' description of concepts well. This was used to understand their perception and behaviour toward IS Security e-competencies development and for building theory.

5.3.2.1 Functionalist research paradigm with reference to Activity Theory

With reference to sociological background, the functionalist research views the society as a system that cannot be studied in isolation. It establishes the existence of the social structure to consider how it functions and its relationship with other parts of the society (Haralambos & Holborn, 1991:9).

According to the description of functionalist paradigm of Burrell & Morgan (1979:26), it seeks to understand society in a way which generates knowledge that can be put to use or provide practical solutions to pragmatic problems. They believe that human experience of the world is subjectively discoverable, and assumes that there are external rules and regulations governing the external world (Ardalan, 2010) that is observed, and which the observer needs to follow.

In relation to its mother body (the positivist approach), which Haralambos & Holborn (1991:17) link to behavioural matter that can be measured such as temperature and pressure, methods of objective measurement can be devised for human behaviour. Such measure is essential to explain behaviour and to produce statements of cause and effect. This reflects the central element of positivism, which is the explanation of social phenomenon by observing its cause and effect (Henn, et *al*., 2009:14).

A functionalist approach (Haralambos & Holborn, 1991:9) coupled with the Activity Theory (explained in Chapter Two) became handy in identifying the constructs

(subjects, tools, object, rules, community, division of labour, and the outcome) that interact and intermediate the interaction in the given environment (in this case HEI) to achieve the object of the activity (development of IS security e-competencies among the subjects, the latter representing IS resources end users).

5.3.2.2 Interpretive research paradigm

The interpretive paradigm is associated with the active way of learning about the social world or phenomenon (Henn et *al*., 2009:15-17). According to the interpretive belief, it is not the external factors and measurable processes that determine human behaviour in the social world; however the meanings people have of the world. Punch (2014:17) explains that the meaning that end users associate to IS resources security can dictate their behaviour toward the IS resources security. This refers to subjective interpretation (Burrel & Morgan, 1979:28) and seeks to create infinite solutions and alternatives to the understanding of the social world as participants describe and not the observer of the action.

The interpretive paradigm's view of the world is in line with the aim and objective of this study due to its collection of participants' point of views (experts and general end users) related to IS resources security (Rastogi & von Solms, 2012). Also, IS security e-competencies development is not only an applied social science, but its impact is also influenced by the way it is described, and positioned in the social context (Avison & Pries-Heje, 2005:191). In this regard, the impact of IS security e-competencies can be described by interpreting end users views and behaviour, but also observed and measured according to the practices of a particular HEI (Burrel & Morgan, 1979:28).

Given the requirement for end users to interpret and participate in the IS resources security compliance (legal, procedures, policies, and controls), researchers (White & Dhillon, 2005 as cited in Rastogi & von Solms, 2012) suggested the use of the interpretive paradigm in solving the IS security issues. In this regard, the approach to IS security is holistic and end users are drawn in the process to "*learn, adapt, and accept the IS security controls and policies*" (Rastogi & von Solms, 2012).

5.3.3 This study and research paradigm

To position this study on a specific philosophical perspective, it is important to reflect on what knowledge and if it can be discovered in information systems security with reference to ontology and epistemology.

The assumption about reality, in terms of reality (ontology) and the science of knowing and how it can be obtained (epistemology), (Gilbert, 2008:138) social research prompted the researcher to ask if the IS security e-competencies development is a reality that can be measured objectively (ontological positivist) or if it is socially constructed based on the researcher's interpretation (ontological interpretive). Furthermore, it had to be determined if the output of the IS research, be it a product such as a software, hardware, and training (such as IS security e-competencies development as the case of this research) is measurable and that the impact is measured in real context or through the support given to other processes of the organisation.

On the epistemological background, positivists believe that the purpose of social research is to develop abstract and general theories about how the world works and test hypothesis. The interpretive on the other hand, seek explanation and understanding; they tell stories (Gilbert, 2008:138). These views are consistent with Burrel & Morgan (1979:21-28).

Positivists draw more commonly on quantitative research but some positivists also draw on qualitative data (Punch, 2014:16). However, positivistic purist spurns studies that draw on a small number of cases because they can never be representative and offer limited possibility of generalisation (Johnson & Onwuegbuzie, 2004; Gilbert, 2008:138). In this study, the researcher opted for a mixed research approach, instead of relying on either quantitative or qualitative data. This was to avoid the limitation of generalisation of results (Gilbert, 2008:138). It is also a non-purist approach, which enabled a form of interdisciplinary research (IS resources security, and education and skills development or training and development) to increase the complementary nature of the methods and answer this research questions (Johnson & Onwuegbuzie, 2004).

This study follows a functionalist research paradigm as the leading approach of knowledge discovery. This is evident in the belief in the existence of the objective world of IS security and e-competencies development, which is not based on the researcher's own interpretation. Furthermore, it is the research's intention to develop a working model that can support the identification and supply of IS security e-competencies. However, due to the differentiation in environment and context in which end users and their organisations are situated, the interpretive approach was referenced to the contextual IS e-competencies (according to that environment). Hence, the functionalist-interpretive approach was used.

The functionalist-interpretive approach therefore recognises the importance of the societal constructs and their interaction in the development of IS security e-competencies. Nonetheless, the important role of end users and their willingness to learn and apply the knowledge in the protection of IS resources is acknowledged. These two important paradigms are well studied under the Activity Theory (AT) which recognises the context of the society in which the activity is studied and helps in the identification of the constructs as they interplay to achieve the object.

The functional-interpretive approach to e-competency development in this research was intended to review the application of IS security measures from human perspective. A further purpose was to identify practical ways of improving end users' security e-competencies and including them in the formal IS security strategy and programme in the HEI environment.

Despite the view of White & Dhillon (2005) as quoted by Rastogi & von Solms (2012) who proposed the shift from functionalist to interpretivism, the functionalist paradigm has been selected as the leading approach for this research. This is because IS security relies heavily upon end user interpretation and participation in compliance with IS security policies and controls in the organisation. The field of IS security and IS security e-competencies development are real and applied in the field. Hence, a solution needs to be developed for the identification and supply of relevant IS security e-competencies.

However, due to the qualitative research approach, the different contexts in which users and their HEI were located, the interpretive approach was used to translate the understanding of the objective world of IS security into the context of end users' environment. The intention in this instance was to create a security environment that does not exclude end users and their views. Therefore, the paradigm for this research is functionalist-interpretive to draw from combined benefits of understanding, interpreting, and recommending a solution applied in the real social environment.

5.3.3.1 This research stance

Quantitative and qualitative research designs can be used to study a phenomenon of interest such as the study of IS security e-competencies development in the selected HEIs. The difference according to Gilbert (2008:35) is that the quantitative research aims to create a numerical description of the phenomenon, perhaps through a process of 'coding' verbal or textual data. While in qualitative research, the researcher aims to create an account or description without numerical scores.

To complement the short falls of qualitative and quantitative research, this study adopted the mixed research approach as its underlying research method. Under the mixed method design, every element of research such as background to the problem and review of previous research, methodological approach, methods of data collection and analysis were planned and considered (Gilber, 2008:58).

To understand what mixed research method is, Tashakkori & Teddlie (2003:711) as cited by Teddie & Tashkkori (2009:7) define it as the type of research design in which qualitative and quantitative approaches are used in questions, research methods, data collection and analysis procedures and/or inferences. This combination is needed to achieve breadth and depth of understanding the research phenomenon (Johnson et *al*., 2007:123 as cited by Tashakkori & Teddllie, 2010:51).

The assumption according to Creswell (2012:535) is that the use qualitative and quantitative methods combined provide a better understanding of the research

problem than when either of them is used on its own. This leads to the mixed method being seen as complex, difficult, and innovative (Tashakkori & Teddllie, 2010:238).

The advances in mixed research also suggest that a study can still be qualified as mixed method by drawing different types of qualitative data or methods (Cronin et *al*., 2007) cited by Gilbert (2008:127). Alternatively, it can be those bringing different quantitative methods together. On the qualitative front examples include the combination of textual data from interviews of focus groups, ethnographic observations, diary entries, life histories, and historical documents (Gilbert, 2008:133; Avison & Pries-Heje, 2005:223).

In the case of this research, the first stage of contemporary data collection comprised the: a) first phase of interviews with security experts from non-participating HEIs, b) the interviews with security experts from the four participating HEIs, c) the interviews with the training and development department of the participating HEIs, d) interviews with registrars from the four participating HEIs who represent their institutions' highest decision-making bodies and their committees that make IT security decisions, and e) the review of documents pertaining to the research phenomenon. Then a second stage involved a survey with the end users of key IS resources of the four participating HEIs to explore their understanding and the impact of the phenomenon on their work.

The advantage of combining qualitative and quantitative methods in mixed method was helpful for this research as it harnessed the strengths of both methodologies to complement each other (Somekh & Lewin, 2005:215). While the qualitative research allowed immersing in the detail as a result of interaction and interviews and other means of data collection for the purpose of theory building and understating IS security e-competencies in the HEIs, the quantitative research assisted in testing the theory (Cooper & Schindler, 2006:198).

Apart from its increasing popularity as a means to harness the strengths of qualitative and quantitative research methodologies (Somekh & Lewin, 2005:215), the mixed research method also helps the researcher to know more about the topic

that is investigated, help to increase accuracy of research findings and the level of confidence in results, help to generate new knowledge through a synthesis of the findings from different approaches, and help to demonstrate theoretical claims that knowledge is both qualitative and quantitative (Gilbert, 2008:127).

The qualitative research stance was found a beneficial choice for investigating topics of sensitivity and complexity like IS resources security, and privacy applied across various entities. The reasons being that it has the prospect of discovering rich context related to the study (Zafar, 2013; Whitman, 2004) as participants are reluctant to indicate the exact state of their IS security for it may make them vulnerable in their use of IS resources (Whitman, 2004).

There are many purposes for conducting a mixed research and researchers need to know the reason of conducting mixed research apart from it being a research method. Among the purposes, Venkatesh et *al*. (2013) mention a few advantages, namely its complementary nature, completeness, developmental, expansion, corroboration or confirmation, compensation, and diversity.

There are many objectives accomplished through a mixed method. Creswell et *al*. (2003) as sited by Maree (2007:261) mentions the following four objectives:

1. Explain or elaborate on quantitative results with qualitative methods data.
2. Use qualitative data to develop a new measurement instrument or theory that is subsequently tested.
3. Compare quantitative and qualitative data sets to produce well-validated conclusions.
4. Enhance a study with a supplemental data set, either quantitative or qualitative.

This research purpose of conducting mixed research was to complement. This is because survey data from end users on IS security e-competencies development in the HEI was used to obtain additional insights on the interviews conducted with IS security experts and other communities of interest from participating HEIs.

The selection of mixed method was also because of the nature of the research problem, research objective and research questions (Creswell & Clark, 2011:267-268; Johns, 2006 as cited in Venkatesh et *al*., 2013). Also, the choice of a mixed method was based on the need for a holistic approach to understand IS security e-competencies development, drawing from the expertise of participants inside and outside of the four participating HEIs and end users, which could not be satisfied by one research method.

In the case of this research, the mixed method is used with the objective to enhance the understanding of the topic by supplementing quantitative research data with the qualitative data that were collected through interviews. This choice is in line with the answers to questions of Maree (2007:274), indicating that an answer of yes to the following questions will indicate a mixed method as the preferred choice:

1. Are there advantages, for your study, to collect data that involves a large number of people and can be representative of those people (i.e. quantitative data)?
2. Are you providing information about specific views of individuals or about your observations while or after a site visit that present the actual research problem as experienced by individuals (i.e. qualitative data)?

To the above questions, the views of Hennink et *al*. (2011:16) and Cooper & Schindler (2006:198) may also be added to support the selection of an approach to method. The authors say that the purpose of qualitative research is to understand the questions: why? how? what? An example of such a question would be: *"What are the influences or contexts?"* This opposes the quantitative research where the purpose is to measure, count and quantify a problem. In quantitative research, answers should be obtained for questions like: how much? how often? how many? These questions are in line with this research questions and those presented in theoretical framework in Chapter One (Figure 1.1).

5.4 POPULATION AND THE SAMPLE

The identification of population and the sample to a research project is considered to be the first step in the process of collecting quantitative data (Creswell, 2012:141).

The decision in the context of this study was whether to include individuals or entire organisations or a combination of the two. The decision also included the number and quality of participants, which was aligned with the aim and objective of this research.

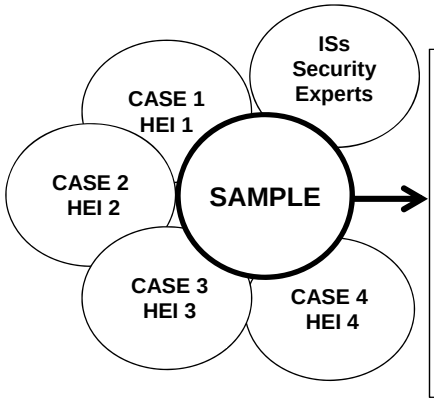
5.4.1 Population and the study sample

In general, the research population represents a group of participants with whom the researcher conducted interviews, administer questionnaires, and observed participants' actions and practices in line with the research aim and objectives. According to Creswell (2012:142) and Dunn (2010:154), this population forms a group of individuals who have the same characteristics. The sample is, on the other hand, a subset of the whole population which is actually investigated and whose characteristics can be generalised to the entire population (Bless & Higson-Smith, 2004:84; Walliman, 2005:277). The basic idea of sampling is that by selecting some of the elements in a population, a researcher may draw conclusions about the entire population (Sahu, 2013:56-64; Card, 2012:34-36; Maree & van der Vesthuizen, 2009:23).

In this research, the sample from which the data was collected was separated into two classes that were also related to the data collection phases:

- The first class represented the IS security experts from the non-participating universities in South Africa who are knowledgeable about this research topic (e.g. lecturer on the topic or researchers). This sample was useful as it helped to collect data on the research topic and also helped in clarifying the current status quo at a number of the South African HEIs.
- The second class represented the sample from the four HEIs studied in the Western Cape Province. This sample included the top managers (e.g. registrar), the IS security manager, the legal representative, and the training and development representative of each institution. They were labelled as the IS security interest group since their positions have a relevant link to the IS security e-competencies development. After the interviews were conducted with this sample, the researcher was able to identify the appropriate sample of

key end users to whom the survey was administered as shown in Figure 5.1 which presents a summary of the sample of the participants to this research.



- ISs experts from other HEIs = 10 Interviews
- Registrars from participating HEIs = 4 Interviews
- ISs security officers from participating HEIs = 4 Interviews
- Training and development representatives = 4 Interviews
- Legal officers from participating HEIs = 5 Interviews
- End-users from participating HEIs = 385 surveys

Figure 5.1: Research population and sample

(**Source**: Adapted from Creswell, 2012:142, Lapan & Quartaroli, 2009:255)

Somekh & Lewin (2005:218) believe that the crucial factor with sampling is the absolute size of the sample rather than the proportion of the population sampled (relative size). They believe that the larger the sample size is, the smaller the error is in estimating the characteristics of the whole population. These authors recognise that the size of the sample depends on the study being conducted. For example, 30 participants for correlation studies and 30 for each group in experimental designs can be considered as a good sample (Somekh & Lewin, 2005:219).

Quantitative and qualitative research present different perspectives in the size of a representative sample (Gray, 2014:225-233; Kumar, 2011:20; Lapan & Quartaroli, 2009:254-255). Quantitative research requires a large sample for the application of statistical inference while the qualitative research requires a small sample because of the time, money, and labour involved in its collection and analysis. Avison & Pries-Heje (2005:246) agree that one in-depth case study is sufficient, if done well.

This research's sample was selected into two phases. As already mentioned, the first phase of this research's sampling focused on the experts from the non-participating HEIs, then the four cases (participating HEIs). In accordance with the rules for the mixed method sampling (Teddlie & Tashakkori, 2009:181), this study

used convenience sampling (nonprobability or purposive) given the perceived easy access to participants.

5.4.2 Sampling tools and techniques

Sampling techniques are traditionally subdivided in two main groups, namely the probability (random) sampling and the nonprobability (purposive) sampling (Creswell, 2012:143; Somekh & Lewin, 2005:216:217; Bless & Higson-Smith, 2004:86-93).

The probability sampling was used in this research for the survey, which gave every member of the target population (key end users identified during the interviews) the same chance of being selected and it was mostly associated with the quantitative research (Creswell, 2012:142-143) and (Lapan & Quartaroli, 2009:254). It included the following strategies:

- Simple random sampling: It was used at one participating HEI which provided a list of 915 employees from which 500 were randomly selected randomly (Kumar, 2011:203). It was used for questionnaire distribution and provided an equal opportunity to each participant to take part in the survey and the questionnaire was e-mailed to them by the institution.
- Multi-stage sampling: This is a strategy in which two or more stages are followed. The researched started with sampling a population that is more general in the original stage, than the final one. Then, in a second stage, one basis of the first sample, a new population is considered that is less than the first population group. The procedure continues until the population to be investigated or final sample is reached.

The other traditional sampling method is the nonprobability sampling in which the researcher selects the participants because they meet certain characteristics such as convenience and availability. Also, this is an efficient sampling method if the result of the study may not be generalised (Creswell, 2012:145). This strategy is commonly identified with qualitative research (case studies or action research) Somekh & Lewin (2005:219) and the following strategies were applied from the nonprobability sampling method:

- Expert sampling: This technique was used for the selection of ICT security experts, legal services experts, and training and development experts to share information on their respective portfolios and how their practices inform the IS security e-competencies development in their respective institutions.
- Purposeful sampling or judgemental: This technique was applied for the selection of registrars from four participating HEIs due to their knowledge of HEIs procedures, and as they act as secretaries to all the committees of the council and Senate, and they satisfy the purpose of research (Bless & Higson-Smith, 2004:86-93; Lapan & Quartaroli, 2009:90-91). They represent the highest decision making body (council) for each participating HEI on the IS security related decisions and are therefore purposeful.
- Convenience sampling: This technique was used for distributing questionnaires to the end users from the three HEIs (HEI01, HEI02, and HEI03) that ethically cleared this research to collect data from their employees. This strategy was useful to get end users from their offices and ask their permission to participate in the research (Lapan & Quartaroli, 2009:90).
- Snowball sampling: This is a technique to reach potential participants who could not be reached by other sampling techniques. It required the researcher to ask the interviewees to identify and recommend end users in their department to whom a questionnaire could be distributed (Lapan & Quartaroli, 2009:91).

With reference to this mixed method research, Lapan & Quartaroli (2009:255), and Bickman & Rog (2009:291) propose strategies for selecting relevant types of samples. These strategies reflect the combination of random and purposive sampling (Bickman & Rog, 2009:292), which also has an advantage of complementing the strengths of one another. For the purpose of this research, the emphasis is placed on the classification of Teddlie & Tashakkori (2009:185-187) who listed the following four strategies related to mixed method research:

- Basic mixed methods sampling strategies;
- Sequential mixed methods sampling;
- Parallel mixed methods sampling;

- Multilevel mixed methods sampling; and
- Sampling using multiple level mixed method strategies.

For the purpose of this research, the sequential mixed method sampling strategy (Teddlie & Tashakkori, 2009:189) was used. The sequential sampling allowed the use of two samples (the probability sampling for quantitative data and purposive sampling for qualitative data) in sequential form. This form of sampling was important for this research as techniques complemented each other and the findings from qualitative approach were used to inform the quantitative approach (Venkatesh et *al*., 2013). The participants were selected in the following two groups:

- One group (security specialists, staff development experts, legal service experts, and registrars from participating HEIs) were sampled by using nonprobability sampling (qualitative approach), particularly using the expert and judgemental sampling strategies, and through these strategies the IS security experts from the four participating HEIs and additional nine experts from seven non-participating HEIs were interviewed using in-depth interviews.
- The other group (IS resources end users) were sampled by using the combination of probability sampling (quantitative approach), specifically the simple random approach from one participating HEI, the snowball sampling, and the convenience approach, to this group of participant the questionnaires were administrated. Snowball sampling was also used as some questionnaires were distributed as the heads of department (Henn et *al*., 2006:157) and experts in interviews recommended.

The interviews with IS security experts in each HEI revealed assistance in identifying the critical assets with key users who need security e-competencies the most. This was evident in that those participants, to whom questionnaires were distributed, accessed critical assets. The results of the data collected from the four participating HEIs were triangulated (cross-validated) for each research question.

5.5 TECHNIQUES FOR DATA COLLETION AND ANALYSIS

The selected data collection strategies and the techniques for data analysis to reach this research objective, and answer the research question and sub-questions, were the best suited for gathering data from the selected sources.

As with other research in other areas of the social research field, IS research use a variety of data sources for the needed data to create theory, frameworks, and draw conclusion on the research phenomenon under study. Cooper & Schindler (2006:196) suggest that qualitative research draws data from a variety of sources such as:

- People (individuals or groups): In this study, people refer to the IS experts from other HEIs in South Africa, the staff members of the four participating HEIs in the Western Cape such as the registrar, the IS security expert or manager, the staff training and development manager, and the legal department.
- Organisations or institutions: These are the selected cases that were used to conduct field work. The mention of fieldwork is in line with the description of case study in which the HEI is investigated (Welman & Kruger, 2001:183).
- Texts (published): Welman & Kruger (2001:35) highlights the importance of doctoral students to consult their primary source of data in order to be acquainted with the background of their studies. However, it is also important to consult previous publications such as books, journals articles, Laws and regulations published through the government Acts, and internal documents published by HEIs such as IS security policies, rules and regulations, and training related documents and schedules to be updated on the practices in the field of IS security e-competencies development.
- Settings and environments (visual or sensory and virtual material): Even if this study focuses on the end users' IS security e-competencies, environment in which they are working is also studied and observed to understand how it influence their behaviours and practices in relation to their IS security e-competencies development.
- Objects, artefacts, media products (textual, visual, and virtual material): These are referred to in Activity Theory (AT) as the intermediating between the

subjects and the object of the activity. The discussion of these elements is based on their support for the development of the end users' IS security through awareness and training and to see how these artefacts can also be of importance in the development of IS security e-competencies.

- Events and happenings: Events on IS security workshops and awareness, the occurrence of threats to IS resources and the institutions' reaction to security issues can also be of importance for the collection of data.

5.5.1 Data collection techniques

In mixed research, qualitative and quantitative data are collected and analysed to ensure they help in gaining an elaborate approach to the research problem and deepen its understanding (Maree, 2007:261). Data collection in mixed research method can use two strategies according to Teddlie & Tashakkori (2009:246-247):

1. It can be used 'within-strategy' where the gathering of qualitative and quantitative data is collected by using the same data collection strategy; and
2. It can also be 'between-strategies' where the qualitative and quantitative data is collected using more than one data collection strategy.

In this research, the collection of data applied the 'between-strategies' where the qualitative and quantitative techniques strategies were applied as a combined technique. This approach was considered helpful to IS researchers by Venkatesh et *al*. (2013) as interview data (qualitative method) help the researcher to gain rich insights from participants' narrative, while surveys (quantitative methodology) brings breadth to the study and allow for accurate inference.

As for data collection techniques that are related to the qualitative research method, Cooper & Schindler (2006:196) suggest techniques such as focus groups, individual in-depth interviews, cases studies, ethnography, grounded theory, action research, and observation. To this list, Creswell (2012:549) separates the qualitative and quantitative methods of data collection:

1. Qualitative instruments include open-ended interviews, open-ended questions on questionnaires, open-ended observations, documents and visual materials; and

2. Quantitative data applies instruments (e.g. questionnaires, closed-ended interview, closed-ended observation), and documents (e.g. census, attendance records).

From the list of mixed method data collection techniques as Creswell (2012:206-207) presents, the following list is used for this research:

1. Interviews (in-depth): These type of interviews were conducted with the IS security experts from the four participating HEIs, and non-participating HEIs. The purpose was to gather participants' opinions on the importance of this research and practices in the development of IS security e-competencies in their environment and to determine the current research trend in the field. For each participating HEIs, the following managers or their representatives were selected for interviews:
    - The staff development managers: These interviews explored if the selected HEIs are providing end users with training on IS security, the methods used for training, and the challenges they experienced.
    - The registrar: As a secretary to the highest decision making structure in HEI, which is the council and its various committees, these interviews are intended to understand the importance of IS resources and their security to their respective institutions. Also, it is to determine the recent decisions the councils of the four participating HEIs have made through their IS security committees, specifically for the protection of IS resources. Further, interview with the registrar will determine if any decision has been reached related to end users' security e-competencies development.
    - The legal office representatives: They were interviewed also to understand which laws and regulations have an influence on the security of IS resources.

A total of 26 in-depth interviews were conducted, of which 9 were with experts from other HEIs to understand the importance of this research topic and the competencies needed for the end users of IS resources. From the total in-depth interviews, 17 in-

depths interviews were conducted with experts from the four participating HEIs in the Western Cape Province.

Concerning the in-depth interviews with participants, the questions were used as a guideline with flexibility in terms of follow up questions and the order in which they are asked (Henn et *al*., 2006:152). The interviewer applied probing questions to clarify vague responses, or to ask for elaboration of incomplete answers. Such probes varied from “Why?” to “Could you elaborate on this?” which gave the respondents the necessary encouragement to proceed (Welman & Kruger, 2005:161).

As interviews were conducted within a certain time span, time had to be considered. Thus, the interviews were conducted in two phases:

- First phase, were intended for academics from other HEIs who have expertise in and have researched IS security. The purpose of this phase is to clarify the importance of the IS security e-competency development among end users and identify the required competencies and how to best supply these competencies; and
- The second phase of interviews was conducted with the IS security e-competencies development community of interest (registrar, IS security expert or manager, training and development manager, and the legal office) from each of the four participating HEIs. These representatives have an influence on IS security and IS security e-competencies development and practices in the HEI they represent. The influence either stem from their expertise or position in the organisation. Training and development representatives of each participating HEI were also be interviewed to assess their understating strategies for developing and delivery IS security e-competencies in their institution to ensure maximum participation.

During the interviews, the researcher was mindful to not influence the participants’ opinions through his own intention and objectives (Fakeh et *al*., 2012). Also, the participants were given a consent form to assure them of their freedom as

participants to the research and different data collection methods were mixed to avoid bias in the processing of data.

The questionnaires were administered to the end users identified during the interview as key to the security of IS resources to determine their current level of IS security e-competencies, and their willingness to attend IS training and awareness. Furthermore the purpose was to determine the participants' perception on how these IS e-competencies can help them in protecting the IS resources they are using.

The archival analyses were used to review training and development schedules and strategies of the institution. This was done to determine how the four HEIs accommodate the development of IS security e-competencies. Other documents were also analysed, such as security policies and legal regulations like government Acts and institutional rules and standards relating to IS security, IS security e-competencies development, and training and development.

The choice of the above data collection techniques has been supported by the examination done by Bryman (2006) as cited by Gilbert (2008:132), who examined 232 studies that had quantitative and qualitative components combined (mixed research). He found that 57% of those studies had mixed survey instruments (questionnaire or structured interview) on the quantitative side with interviews (semi-structure or unstructured) on the qualitative side.

In general, both methods used in the mixed method (qualitative and quantitative) were represented in the data collection stage. The qualitative data collection ensured that participants, through interviews can express feelings, emotions, motivations, perceptions, language and behaviours in the context of their HEI on the IS security e-competencies development (Cooper & Schindler, 2006:196). The quantitative data included both close-ended and open-ended responses, and observations (Maree, 2007:277).

5.5.2 Data analysis techniques

Cooper & Schindler (2006:196) state that the qualitative researcher can apply content analysis to analyse written or recorded materials drawn from personal expressions by participants, behavioural observations, and debriefing of observers, as well as the study of artefacts and trace of evidence from the physical environment. The useful documents that were used for content analysis in this research include the training schedule, security policies, audit reports, Promotion of Access to Information documents which were collected from the participating HEIs. All these documents were made available or were accessed through the Internet. The critical aspect of content analysis is the unit of analysis (Gamerschlag, 2013).

Speaking on the importance of matching the data collection instrument to the field of information technology (IT), Olivier (2004:100) asks if numbers can be used to express the security of a system or to express the threats posed by various computer viruses. From this study's qualitative perspective, it is important to understand the IS resources security e-competencies from the point of view of the participants in their institutional context (social and cultural contexts), which could be lost when textual data are quantified (Myers, 1997).

Creswell (2012:550-552) stated that in the context of mixed method research, data analysis follows the mixed research design, which can be convergent (quantitative and qualitative data collected simultaneously), explanatory (quantitative data followed by qualitative data), exploratory (qualitative data followed by quantitative data), or embedded (quantitative or qualitative embedded within quantitative or qualitative). According to Teddlie & Tashakkori (2009:252-283), the design can be parallel, conversion, sequential, multilevel, fully integrated, and the application of analytical techniques varies from one tradition to another.

For the purpose of this research and in alignment with the selected mixed strategy and sampling technique, the sequential mixed data analysis (qualitative to quantitative analysis) was applied. In this analysis, the qualitative data were analysed independently from the quantitative data to answers a particular research question. The purpose was to conduct the second analysis (quantitative analysis) to

confirm or not to confirm qualitative data, and to have additional information complementing the first analysis (Teddlie & Tashakkori, 2009:274).

5.5.2.1 Quantitative data analysis

For the analysis of quantitative data, Teddlie & Tashakkori (2009:256), Henn et *al*. (2009:215-223), and Lapan & Quartaroli (2009:103-130) propose the use of descriptive and inferential statistics, which are used to explore or describe the data in advance of the analysis. While descriptive statistics tend to describe data and their pattern (summary of data) in the distribution, the measures of central tendencies, and relationships, the inferential statistics will show the difference or relationship between the participants from the four HEIs in forms of statistical significance and probabilities of occurrence (Somekh & Lewin, 2005:215,226; Creasley, 2008:10; Lapan & Quartaroli, 2009:103-105).

In addition to descriptive and inferential statistics, the nonparametric statistics were also used, which according to Somekh & Lewin (2005:226) and Creasley (2008:88) are part of inferential statistics and can be applied if the data respond to certain conditions if a non-probability sampling technique was used.

It is important to highlight that the type and characteristics of the data that were collected will inform the execution of a specific statistical test (Lapan & Quartaroli, 2009:112,126). For the purpose of this research, in addition to the frequencies that were used to check the participation and appropriate data capturing, both the descriptive and inferential statistics were run to summarise survey data. These statistics apply measures of central tendency such as mode to assess the frequencies of data. The application of descriptive statistics helped to discover trends and patterns, and to summarise results for ease of understanding and communication in forms of frequency tables, means, and correlation. It applies the Statistical Package for the Social Science (SPSS) data analysis software.

5.5.2.2 Qualitative data analysis

The analysis of qualitative data involves an intense interactive process and interpretation between the researcher and the data to reduce all the collected data

from interviews and content analysis into the meaning of words (Lapan & Quartaroli, 2009:259-260). The analysis of the collected qualitative data in this study was based on strategies of Teddlie & Tashakkori (2009:253-254) such as open coding, contextualisation, and qualitative data displays which are briefly discussed below as they were applied in this research.

5.5.2.3 Open coding

Open or initially developed codes were used to summarise the data, to break down narrative data and rearrange those data to produce categories that facilitate comparisons, thus leading to a better understanding of the research questions through content analysis (Lapan & Quartaroli, 2009:265). It is in the codes that the patterns are collected through repeated occurrences (and also co-occurrences) or other pattern are given by the participants as they see them important of mentioning (called declaration) in respect of this research (Lapan & Quartaroli, 2009:267-270) with intention of developing theory.

Given that the investigation of threats and related security to IS resources presents a threat and intrusion (Zafar, 2013) to HEIs' sensitive assets that cannot be easily shared with the outsiders, this study adopted the content analysis data analysis strategy. This content analysis can be used as a single data analysis strategy when investigating the trends from multiple articles (Cooper & Schindler, 2006:449) and other official documents such as legal Acts and internal regulations, security, and training policies related to IS security and IS security e-competencies development.

5.5.2.4 Contextualisation

This holistic strategy was used to interpret the narrative data in the context of a coherent, whole "text" that includes interconnections among statements, events, and so forth. The focus is on the entire experience rather than a specific component. Techniques such as narrative analysis and ethnographic analysis are among those in this strategy.

5.5.2.5 Qualitative data displays

These are visual presentations of the themes that emerge from the qualitative data analysis which helped in summarising information from either categorisation strategies or as a separate data analysis scheme. Techniques such as effect matrices and concept or mental maps are among the different techniques used in this study. For this purpose, the study made use of the analysis software Atlas.Ti.

These strategies were used within the Grounded Theory Methodology (GTM) for identifying and development of categories and their properties, which are explained as "conceptual" aspects of categories (Glaser & Strauss, 1967). In this study, according to the advice of Croswell (1998) and Dey (1999:1-2), qualitative data analysis began as soon as data were available. This is done by constantly comparing analysed data with the developing categories and their properties.

Data analysis proceeded from 'open' coding (identifying categories, properties and dimensions) through 'axial' coding (examining conditions, strategies and consequences) to 'selective' coding around an emerging storyline, followed by memoing and sorting findings (Glaser & Strauss 1967; Glaser 1978; Glaser 1998; Charmaz, 2006; Urquhart, 2013:23-24; Lichtman, 2010:190). The result of the application of GTM in this study, coupled with the quantitative analysis, was through inductively generating a tentative but explanatory theory about the phenomenon researched (IS security e-competences) (Johnson & Onwuegbuzie, 2004).

This approach of using GTM only for data analysis is based on works of a number of modern grounded theorists who suggest that the basic GTM guidelines, given by Glaser & Strauss (1967) can be used with the contemporary methodological approaches as done in this research (e.g. Bryant & Charmaz, 2007; Clarke, 2005; Mitrovic, 2008).

5.6 Data validity and security

The application of triangulation which merges mixed methodologies and data collection techniques (Venkatesh et *al*., 2013) helped in answering the research

questions of this study and also enforces the validity and reliability of the collected and analysed data (Somekh & Lewin, 2005:275).

This research has also referred to additional approaches for validating data to avoid mismatch between triangulation with some forms of qualitative research, mainly interpretive (Willis, 2007: 220; Henn et *al*., 2006:214). For this purpose, the research questions for interviews and questionnaires were first discussed with the supervisor, and tested through a pilot step with ten respondents (in the case of survey) to evaluate if they can be understood without ambiguity. The in-depth interviews used similar questions in questionnaires that were asked in different ways to improve on the question of validity (Henn et *al*., 2006:214). The additional approaches for ensuring validity are peer reviews.

To ensure excellence and relevance, this research's draft chapters and ideas were subjected to a constant peer review with peers in the faculty and experts in the field for their opinions, suggestions for emerging trends, and guidance towards the conclusion (Card, 2012:3; Tim, 2011:52). With reference to research journals, the researcher ensured that all the ideas and thinking emerging during the process are recorded; reviewed and reflected upon to guide the thinking towards and conclusion (Ardoin et *al*., 2014; Willis, 2007: 220).

Given that this research engaged with institutions and individuals whose details and information need to be protected from unauthorised access and use, security measures such as locked cabinet (for printed and other recorded files) and password protection (for digital form) were used to ensure that no person external to this study accessed them. When the final document has been published, these documents were destroyed (burned or shredded) to prevent misuse and access without consent of the initial participants.

5.7 CHAPTER SUMMARY

This chapter described the design and methodology followed to conduct the investigation on the IS security e-competency development and the development of a theoretical framework for e-competencies development in the higher education

institutions (HEIs) environment. For this framework to be developed, the mixed method was identified and selected as appropriate for conducting this research and enrich the research by drawing from the strengths of combined methods and minimise the weaknesses of a single method.

For the research strategy, a multiple case study was selected. In this strategy, four HEIs in the Western Cape Province were selected to participate in this research with the aim to investigate IS security e-competencies practices using in-depth interviews in two phases: first with the IS security experts from the non-participating HEIs, then with the IS security e-competencies development community of interest (top managers, IS security expert or manager, training and development manager, and the legal office) from the four participating HEIs.

After the interviews, a survey was conducted with the sampled key end users for whom IS security e-competencies are important in the protection of IS resources. In addition to strategies for primary data collection (interviews and surveys), an extensive content review was also conducted to review the trends in the IS security and e-competencies development, the participating HEIs practices on IS security e-competencies development, and the effects of legal requirements, security policies, and other internal requirements on IS security e-competencies development.

The next chapter presents an analysis of primary and secondary data collected for the purpose of this research and how the content analysis, grounded theory, and descriptive statistics were applied for their analysis.

CHAPTER SIX: DATA ANALYSIS

6.1 INTRODUCTION

The data analysis presented in this chapter followed the principles of mixed method research presented in the research design chapter (Chapter 5). During the data analysis, both qualitative and quantitative data analysis techniques were kept separate for each research sub-question to respect the principles of each technique, the nature of knowledge, and the nature of empirical data collected as each relates to the research objective and question (Creswell, 2009:12; Henn et *al*., 2006:213-214) to keep the nature of each empirical data.

In relation to the flow of the analysis for each research sub-question, the qualitative data collected through in-depth interviews were analysed first. Thereafter, they were supported by the quantitative data that were collected from the survey as they relate to that particular research sub-question. The interviews conducted with nine experts from seven HEIs across South Africa were first analysed in order to assess the relevance of IS security e-competencies to be developed among the end users in the HEI environment. Then the empirical data from the four HEIs in Western Cape Province were done to answer the research question.

To ensure consistency in this chapter, the word Information and Communication Technology (ICT) is used for the analysis to replace the word Information Technology (IT) even if the participants use the latter word. In most cases, even the words information, data, hardware, and software themselves are replaced by ICT as they are components of ICT.

The grounded theory and content analysis approaches were applied for the analysis of qualitative data with the help of Activity Theory (AT) which was used for the categorisation of data and grouping of codes according to the AT components. In this way, AT fulfilled its role of being the lenses for the analysis of IS security e-competencies development activity in the four HEIs investigated. Apart from the object or purpose category of IS security e-competencies development, other

components of AT such as subjects, tools, rules, community, and subdivision of labour were used as the lenses for the categorisation of qualitative data.

6.2 INTERACTION WITH EXPERTS ON IS SECURITY E-COMPETENCIES

The data from experts were collected to affirm the importance of the object or purpose category. They were selected based on their knowledge of the research topic and were identified after reading their published articles, a review of their profile on the website of the university they are affiliated with or inquiry in their department. For this purpose, Table 6.1 presents a coded list of experts and their HEI of affiliation.

Table 6.1: Experts and university of affiliation

Higher Education Institution	Expert	Data collection technique and approximate duration	Province / City
HEI05	3 Experts (EXP07, EXP08, EXP09)	Interview (Recorded, 1 hour x 3)	Johannesburg
HEI06	1 Expert (EXP10)	Interview (Recorded 1 hour)	Pretoria
HEI07	1 Expert (EXP11)	Interview (Recorded 1 hour)	Johannesburg
HEI08	1 Expert (EXP12)	Interview (Recorded 1 hour)	Johannesburg
HEI09	1 Expert (EXP13)	Interview (Recorded 1 hour)	Pretoria
HEI10	1 Expert (EXP14)	Interview (Recorded 1 hour)	Port Elizabeth
HEI11	1 Expert (EXP15)	Interview (Recorded 1 hour)	Limpopo
TOTAL	**9 Experts**	**9 hours**	

6.2.1 Experts' views on IS security e-competencies development: Object or purpose component of Activity Theory (AT)

When asked about the importance of the security training to end users, one expert (EXP14) at onset expressed that "*everybody knows there is problem and beside that lot has been spoken about the topic, it has not been solved yet".* Be it from governance, technology, risk, or education's point of view, the fact remains that a problem exists. But the question is "*how are we going to solve the problem? Now*

that you are looking at various e-competencies levels and I agree with you given that there are a lot of responsibilities and there is very little proven success in this area".

Referring to the innovation in both ICT infrastructure and related threats which change the scope of security, the expert (EXP14) continued to say that "*we know that the target is a moving target, and technological controls alone are not going to solve the problem, because there is human aspect associated technology be it locking, password, firewall or any other control, therefore humans (end users) need to be at a certain level in ICT security".* In relation to this research, it is a matter of what people need to know and how you are going to offer it to them that matters and for this knowledge to occur certain elements of education need to be involved.

From the interviews with experts, a number of themes emerged that relate to the importance of the object of IS security e-competencies development:

- Not just like a domain of information security specialists;
- Both my responsibility and the institution;
- Attend the training but I will love also to be involved in the training;
- I will support training;
- Training of end users on IS resources security is very important;
- To attend and support;
- I will support the IS security training and awareness; and
- Everyone needs IS security training and skills.

Table presented in Appendix H summarises the views of experts on the category object of the IS security e-competencies development.

Apart from the importance of the IS security training and the development of IS security e-competencies, one IS security expert (**EXP14)** clearly indicated that "*ICT security culture is fairly new and it cannot be passed from one generation to another, the IS security education should play a critical role in not only building IS security skills but also developing IS security culture".*

To support the interview data, the experts were also given a survey to support their responses expressed during the interviews and are presented in Tables 6.3, 6.4, and 6.5. The last two tables (Table 6.4, and Table 6.5) are also addressing the analysis of rules and tools of Activity Theory (AT) that support the achievement of the object of the activity system, which is to develop the IS security e-competencies of the end users.

Table 6.2: Experts' views on the importance of security training for end users in the protection of IS resources?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Important	9	100.0	100.0	100.0

Table 6.3: Experts' view of the importance of a security policy for the protection of IS resources?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Important	9	100.0	100.0	100.0

Table 6.4: Experts' view of the importance of the security culture important for the protection of IS resources?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not Important	1	11.1	11.1	11.1
	Important	8	88.9	88.9	100.0
	Total	9	100.0	100.0	

On the content of IS security e-competencies development (ICT security training), the experts from other HEIs (and the four participating HEIs) suggested the content as stated in Table 6.6 below. Important to mention is that the content of IS security e-competencies development for end users has been grouped into the following four spheres of IS resources security as mentioned in Tshinu et *al*. (2014). It is important to also mention that the majority of the topics are non-technological measures.

Table 6.5: Content of ICT security e-competencies development

IS SECURITY SPHERES	IS SECURITY E- COMPETENCIES
ICT security policies and procedures	1. Importance of IS security in HEI environment. 2. E-mail and their attachment (do not open any unknown e-mail or attachments, careless e-mailing and forwarding confidential information). 3. Knowledge of ICT policy and the user guideline in your organisation. 4. Password and Access details management (selection, complexity, carelessness, sharing, renewal, and management). 5. Knowledge of their roles and responsibilities. 6. Knowledge of security threats and risks (phishing, spam). 7. Security on exam paper and their handling of other critical information. 8. Ownership and responsibilities for information and IS resources you access. 9. Knowledge of the implications of their actions (not logging off). 10. Responsibility in reading communications and policies. 11. Managing of user environment (disclosure of information, and informing the manager on suspicious activities, handling power failure). 12. Leaving staff/students cards around. 13. Storing information on non-secure locations. 14. Carrying laptops of campus, leaving in car. 15. Dealing with confidential information in open office /area. 16. Printing confidential documents on a shared printer. 17. Filing confidential information in a wrong location. 18. Unthinkingly sharing confidential information. 19. Know how to use computers. 20. Using shredders for confidential information. 21. Know that the PCs contain valuable information and data. 22. Scan your PCs for any potential virus after downloading any application from the Internet. 23. Information and data criteria (Confidentiality, Integrity, and availability). 24. Not to divulgate the information like student marks. 25. Locking of offices and cabinets. 26. Information curator to annually certify who review the access to information in their system.

Environment (internal and external)	1. Confidentiality, integrity, and availability (CIA) of information and related resources. 2. The end user ability to establish and manage the security of IS resources. 3. Knowledge of legislation and regulation such as Impact of acts such as POPI, ECT, and PAI on IS security. 4. Be aware of what is legally right and wrong (in law you cannot say you do not know, you cannot download pornography and say you do not know). 5. Do not abuse your resources, like do not watch movies. 6. Importance of respect for physical security (Security guards). 7. Be aware of social engineering. 8. Be aware of shoulder surfing. 9. Be aware of phishing / Spam / Hacking. 10. Fear of exam paper being compromised because they are on the network. 11. There is always that possibility of stealing IT equipment in the area where there is no proper environmental management. 12. The management of user environment, that is if you do not regard it as your ATM card there is something wrong. 13. Leaving staff/students cards around. 14. Locking rooms and offices. 15. Make them aware of the risks if we do not follow the good practices. 16. Filing confidential information in a wrong location. 17. Exposing university resources to viruses risks (e.g. children play on work laptop). 18. Be informed about the classification information and IS resources. 19. The implications of compromising security (degree of discipline IS if you breach the security of IS resources).
Basic security technologies	1. Basic security configuration and controls. 2. Installation of firewalls and antivirus programmes. 3. Update of application software and antiviruses. 4. Scan your portable devices before the transfer of data to your PC. 5. Scan your PCs for any potential virus after downloading any application from the Internet. 6. Technophobes – fear of technology. 7. Avoid flash memories from external environment. 8. Knowledge of implemented certification and authentication

	systems. 9. Be aware of security cameras. 10. Be aware of online monitoring tools. 11. Be aware of threats from open access.
IS security culture	1. Check source of e-mail before opening. 2. Logging off and closing office when going out of the office (never leave your PC unattended for long hours). 3. Compliant security behaviour (compliance to physical and other requirements). 4. Check or do not accept the flash drive from external people and students. 5. Be aware of threats and vulnerabilities to IS resources. 6. Reading ICT security policies and other communications. 7. Avoid careless attitude about physical access. 8. Unthinkingly sharing confidential information. 9. Protected question papers with a password before they are sent via e-mail or when it is stored on your laptop. 10. Visitors need to sign when accessing the campus (management of visitors). 11. Never write down your password or share it. 12. Importance of security culture.

The views from the experts reveal also that HEIs are still vulnerable from exploitation especially from human attitude threats and has its unique challenges that are different to other business organisations (Ahlan & Lubis, 2011). In fact, challenges in the protection of IS resources in HEIs are different to some extend of the other business organisations. Among the challenges that experts mentioned, the following were included:

- The openness to the adoption of new technologies and use of social network sites such as Facebook, and YouTube to promote the interaction between students and academics. Also, the distribution of study materials using the channels that students access and use the most.
- In some cases, HEIs download, develop, and test virus software as part of learning. In business organisation, the social websites are considered as counterproductive and totally blocked or are allowed only after hours. The organisations do not test or create virus software even for learning purpose.

As such, HEIs challenges in protecting their IS resources are higher than those of ordinary businesses.

After the discovery of the importance of IS security e-competencies development from the experts' perspective, the section below focuses on the analysis of empirical data collected from the four HEIs (HEI01, HEI02, HEI03, and HEI04) in the Western Cape that agreed to participate through the representatives from different departments namely the registrar's office, ICT manager or security experts, legal services, training and development, and end users.

From the experts' views, the common theme was that IS security e-competencies development is important in the modern HEIs and needs to be integrated in the operations of the HEIs. This is necessary as the IS resources are integrated in their operations. Armed with this support, an initial pre-research investigation was conducted to discover the practices of IS security e-competencies development in the selected four HEIs in the Western Cape Province.

For the purpose of the analysis, it is important to outline that a total 17 in-depth interviews were conducted with participants from the four HEIs. In addition 9 in-depth interviews were conducted experts from other universities across South Africa. They were identified as key stakeholders in the development of IS security e-competencies. In addition, 385 research questionnaires were collected from the end users from three HEIs to support the findings from the interviews. One HEI (HEI04) only granted permission to interviews but not the questionnaires as the research topic was seen as infringing the security of its information and IS resources.

In relation to the analysis, the qualitative findings are presented first with reference to the codes and the themes relate to a particular research sub question and research sub-objective. Only then, they are supported with the quantitative findings and best practices as the experts proposed in the literatures.

6.3 ANALYSIS OF DATA FROM THE FOUR PARTICIPATING HEIs

This section presents and interprets the data collected from the four HEIs (HEI01, HEI02, HEI03, and HEI04) that officially participated in this research. It starts by presenting the profile of participants and the brief landscape of the cases. It then moves to present the data from the four interviewed HEIs and the quantitative data collected from end users from three HEIs that participated. One institution (HEI04) could not allow the administration of the questionnaires on the basis that the nature of this research could negatively impact on the security of their IS resources.

6.3.1 Presentation of cases (Include the participating HEIs)

The HEI landscape in South Africa is composed of institutions grouped in different units. Namely, the so called traditional universities, the comprehensive universities which combine the nature of traditional and universities of technology, and universities of technology he latter being the result of the transformation of previous Technikons. All these forms of universities present no differences from the context of this research that can motivate their separation as they have similar governing structures and rely on ICT resources to support their administration, teaching and learning, and research.

Beside their structure, these institutions of higher learning have an option to the mode of delivering education, which can be contact mode, distance, or combined learning which merges the aspects of distance and contact modes. In all the above forms (category and mode of delivering education), the ICT infrastructures play a critical role and are embedded in the teaching and learning, research, and general administration of all these institutions (Johl, et *al*., 2013).

For this research, three traditional universities and one university of technology participated in the research and are represented by the codes HEI01, HEI02, HEI03, and HEI04.

6.3.2 Analysing data collected from the four participating HEIs

Before the presentation of the actual data analysis, it is important to know the demographic profile of the participants. This is set out in detail in Appendix E that

presents the various sections of the participating HEIs, the different levels of qualifications that participants hold, and the gender representation.

For the purpose of empirical data analysis, the questions are discussed according to the three categories (research sub-objectives) discussed in Chapter One (section 1.4.2) which are:

1. The exploration of the importance of IS resources and their security in the HEI environment.
2. The exploration of IS security e-competencies development practices which are the current participating HEIs.
3. The exploration of ways of supplying the needed IS security e-competencies in the HE environment.

In addition to the sub-objectives, the components of Activity Theory (AT) were also associated to the sub-objectives and sub-questions to analyse how the four participating HEIs combine the elements of the activity system into their security e-competencies development practices.

6.3.2.1 Sub-objective 1: The exploration of the importance of IS resources and their security in HEI environment

This sub-objective was associated to the object or purpose of Activity Theory (AT) which is used to develop the IS security e-competencies, and the subjects who are in this activity system the IS resources end users who need to be IS security e-competencies development to protect the IS resources they access. To explore this sub-objective, the answers to the questions related to the importance of IS resources and their security in HEI environment were collected from the interviews and from the questionnaires as well. The questions asked during the interviews were analysed first then followed by the answers from the questionnaires.

QUESTION 1: In this section, the **first question** was to understand the importance of IS resources in the operations of the HEIs. From the qualitative data (interviews), the following themes could be collected:

- *Commercial benefits for the university and the nation, then you have to safeguard them.*
- *ICT resources are core to business of HEI because the entire student administration is managed on ICT platform.*
- *ICT is the anchor to the university and our vision and strategic objectives.*
- *The whole system of examination and graduation is mechanised. ICT is not our core business, but it is core to our business.*
- *ICT is absolutely integral part of the university*.

These themes can be traced from the table presented in Appendix I that references participants and their views or quotations.

QUESTION 2: This sections still addresses the object of activity system. The **second question** explored if the four participating HEIs have classified their critical ICT systems that support their operations as needed for protection.

From the interviews with the ICT managers and their security representatives the following themes were collected in no particular order as systems are not classified:

- HR system, student administration system, the financial system, the leaning management system, and the e-mail system as well.
- ERP system because that is where their finances and students' records are, network infrastructures, the blackboard or e-learning system, the exchange system for e-mail, the personal computers in the labs and Microsoft systems that deal with all elements such as research, academic and administration environment.
- Network system, financial system, the procurement systems, the learning management system, the system that manage the awarding of qualifications, and the research systems.
- Finance system, HR system, student information is extremely important, the order management system (procurement), teaching and learning management system, research management system.
- We have not driven classification.
- No classification has been made in detail.

These themes can be linked to the participants and their quotes in presented in the table under the Appendix J.

From the classification of resources according to their criticality as mentioned in Table 6.8, responses from interviews prove that little has been done to formally classify the ICT resources.

Apart from the qualitative data collected through interviews, questionnaires were also distributed to the end users from the participating HEIs to assess their reliance on IS resources to do their work and their perceived understanding of responsibility to protect them. Tables 6.9 and 6.10 provide the analysis of the assessment.

Table 6.9 illustrates that 382 participants (which is about 99.22%) completed the question and only three (about 0.78%) did not participate. When asked to which extent the participants rely on the ICT resources to do their work, it has been demonstrated that the majority of participants (97.3%) agree and strongly agree combined. This trend is about the same for all the HEIs when considered separately, with HEI01 97.3%, HEI02 97.5, and HEI03 97.3%. This means that ICT resources are extremely important for participants to execute their work and for the operations of the participations HEIs.

Apart from the reliance of the ICT resources to do their work, employees were also asked if they use their own computers and mobile phone devices to access e-mails and connect to the network when they are off-campus. Tables 6.9 and 6.10 provide the summary of the responses from the participants.

From the frequency distribution in cross tabulation (Table 6.9) it can be said that 384 participants (or about 99.74%) answered the question correctly and only one participant (or about 0.36%) did not answer the question. From the responses (total columns) it can be seen that the majority of participants (304 participants – those who agree and strongly agree, about 79.2%) use their computer and mobile devices to access their respective institutions' IS services. Even from the individual

institutions, there is not much difference as 79.1% respondents from HEI01, 76.9% of respondents from HEI02, and 84.1% of participants from the HEI03 agree or strongly agree in answer to the same question.

Table 6.6: Participants' dependability on computer and other IT resources to do their work * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			
			HEI01	HEI02	HEI03	Total
I rely on my computer and other IT resources to do my work	Strongly disagree	Count	1	0	1	2
		% within Higher Education Institution (HEI) Reference	0.7%	0.0%	1.4%	0.5%
	I do not Know	Count	3	4	1	8
		% within Higher Education Institution (HEI) Reference	2.0%	2.5%	1.4%	2.1%
	Agree	Count	28	36	8	72
		% within Higher Education Institution (HEI) Reference	18.4%	22.5%	11.4%	18.8%
	Strongly agree	Count	120	120	60	300
		% within Higher Education Institution (HEI) Reference	78.9%	75.0%	85.7%	78.5%
Total		Count	152	160	70	382
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

Table 6.7: Participants' dependability on own computer or mobile phone to access e-mails and connect to network off the campus * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			Total
			HEI01	HEI02	HEI03	
I use my own computer or mobile phone to access e-mails and connect to network off the campus	Strongly disagree	Count	12	22	7	41
		% within Higher Education Institution (HEI) Reference	7.8%	13.8%	9.9%	10.7%
	Disagree	Count	10	9	2	21
		% within Higher Education Institution (HEI) Reference	6.5%	5.6%	2.8%	5.5%
	I do not Know	Count	10	6	2	18
		% within Higher Education Institution (HEI) Reference	6.5%	3.8%	2.8%	4.7%
	Agree	Count	35	39	10	84
		% within Higher Education Institution (HEI) Reference	22.9%	24.4%	14.1%	21.9%
	Strongly agree	Count	86	84	50	220
		% within Higher Education Institution (HEI) Reference	56.2%	52.5%	70.4%	57.3%
Total		Count	153	160	71	384
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

Table 6.8: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	11.101[a]	8	.196
Likelihood Ratio	11.411	8	.179
N of Valid Cases	384		

a. 2 cells (13.3%) have expected count less than 5. The minimum expected count is 3.33.

The end users dependability on IT resources (Table 6.9 and Table 6.10) is also confirmed in the Chi-Square table (Table 6.11) which has a value of X2 = 11.101, df=8, and p = 0.196 p > 0.05. This result means there was not a significant difference in the responses from the participants and that the usage of own computer or mobile phone to access e-mails and connect to the network off the campus across the participating HEIs. In other words, the reflection on the selection of agree and strongly agree was relatively the same from the participants even if they are from different institutions. This result means that the understanding of importance, usefulness of IS resources in supporting HEIs employees in doing their work, and the need for responsibility for the security of these resources extend beyond the on-campus usage to the off-campus use wherever the employees are accessing these services. This includes at home and when they are attending conferences nationally and internationally.

Question 3: The third question asked the participants whose responsibility is it to protect the ICT resources?

While the ICT security experts from the participating HEIs believe that end users are important in the protection of ICT resources, this question was also asked to the end users to explore how they perceive their responsibility in relation to the security of IS resources. Responses are presented in the Table 6.12.

Table 6.9: Participants' view on their responsibility towards IT resources security * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			
			HEI01	HEI02	HEI03	Total
How do you perceive your responsibility in relation to IT resources security?	IT resources security is not my responsibility	Count	23	30	10	63
		% within Higher Education Institution (HEI) Reference	14.9%	19.0%	14.1%	16.4%
	IT resources security is my responsibility	Count	48	51	13	112
		% within Higher Education Institution (HEI) Reference	31.2%	32.3%	18.3%	29.2%
	IT resources security is the responsibility of IT technicians	Count	70	71	15	156
		% within Higher Education Institution (HEI) Reference	45.5%	44.9%	21.1%	40.7%
	It is a shared responsibility between end users and IT technicians	Count	13	6	33	52
		% within Higher Education Institution (HEI) Reference	8.4%	3.8%	46.5%	13.6%
Total		Count	154	158	71	383
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

Table 6.10: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	83.631[a]	6	.000
Likelihood Ratio	68.287	6	.000
N of Valid Cases	383		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.64.

To the question of responsibility for ICT resources security, it can be observed that the responses are mixed. From the total column, a relative high percentage of participants believed that it is the responsibility of IT technicians (40.7%) and another group believes that it is not their responsibility (16.4%). Those who believed that it was their own responsibility and shared responsibility between the users and IT technicians was 29.2% and 13.6% respectively.

Even though a higher percentage of participants (46.5%) from HEI03 believe that it was a shared responsibility between the users and ICT technicians, and 18.3% accepted that it is the responsibility of the end users, the participants from other two HEIs view this differently. A 45.5% of participants from HEI01 and 44.9% of participants from HEI02 indicated that the security of ICT resources is the responsibility of ICT technicians, and 14.9% of participants from HEI01 and 19% of participants from HEI02 stated that the security of IS resources is not their responsibility at all. This leaves the 31.2% of participants from HEI01 and 32.3% of respondents from HEI02 to accept the protecting of IS resources as part of their responsibility. A small percentage of participants (8.4%) from HEI01 and 3.8% from HEI02 indicated it as a shared responsibility between end users and IT technicians.

When comparing the result from the three HEIs on the question of responsibility as presented in Table 6.13, the result shows that the p value is less than 0.05 ($p = 0.000$ $p < 0.05$). This means that there was significant difference between the answers from the participants on how they perceive their responsibility in relation to

IT resources security and the HEI they represent. In this difference however, from cross tabulation Table 6.12, it is clear that a high percentage of participants do not accept the security of ICT resources as their responsibility (16.4%). Those respondents indicated it as the responsibility of ICT technicians (40.7%), if combined, was much higher than the rest.

To conclude this section on the importance of ICT resources and their security in the HEI environment it can be said that participants (both from the interviews and questionnaires) believe that the IS resources are important in the operations of HEIs. Not only because they store critical information, but also because the employees who access these systems are also critical to their security.

The literature review confirmed that the security of ICT resources is an old issue which has been amplified due to the reliance on ICT resources (Whitman & Mattard, 2010:2; Jones, 2009) and global network that link trusted and untrusted users who connect to the infrastructure for different reasons. Given that these resources in HEIs carry sensitive and critical information that are important to the operations of HEIs, it is crucial to ensure that protection against internal and external threats. Forceful or human errors are imperative (von Solms et *al*., 2011 Steenkamp, 2011) as in the current network economy no organisation is immune to security breaches (Monk & Wagner, 2009:215; Gillies, 2011). The protection of ICT resources is considered fundamental for any business (Buecker, 2007) and the development of IS security e-competencies through training and awareness is one of the aspects of ICT security management (Tsohou et *al*., 2012).

Apart from their appreciation for the importance of IS resources security in the HEIs, the participants (**SEP01** from **HEI01** and **SEP03** from **HEI02**) have also advised for the classification or categorisation of data (and other IS resources) to make sense of them before applying any encryption or other controls. The responsibility for this classification is on management rather than ICT as it deals with data retention and record management.

6.3.2.2 Sub-objective 2: The exploration of IS security and IS security e-competencies development practices in the participating HEIs

After a review of the importance of IS resources and their security in the HE environment, this section focuses on the exploration of the development of IS e-competencies among the end users of IS resources in the HEIs. In relation to Activity Theory (AT), this sub-objective related to tools and the rules embedded into the institutions' ICT policy that are supporting the development of IS security e-competencies development.

Question 1 in this section asked the participants about their IS security e-competencies development practices in their respective institutions. **Question 2** enquired about the end users' training in ICT security policy. Information on these questions was initially collected during the preliminary stage of this research. The initial pilot investigation of the training schedules of two of the four participating HEIs (HEI01 and HEI03) revealed that no training has been conducted with the end users that related to the development of their security e-competencies.

Starting with interviews, participants mentioned that no formal training has been provided to the end users that directly related to the development of there IS security e-competencies. However, responses indicated training on access control and the mentioning of the importance of password management during other training for example in the use of the student management system and Microsoft Office.

During the interviews, the following themes were collected from the participants' views:

- In the distant past made it part of induction programme and had a voluntary security awareness coupled to e-mail training in the past.
- The practice fallen away because it was not compulsory.
- The institution falls short on policy training and awareness.
- No training has ever been provided at their institution on ICT security policy.
- The institution has not provided IS security training.
- The coherent training exercise should be done.
- We do not run security training per say.

- We incorporate some aspects in the normal software training.
- Information during the security campaign, antivirus and identity management are provided on the institution website.
- ICT security awareness and training are critical but these are the things the institution has neglected.
- The big problem with the current induction programme is that there is no slot for IT exposure.
- No formal training on ICT security has been done.
- ICT security policy does not prescribe for training on IS security.

These themes can be traced from the table in Appendix K which presents the references and quotes from the participants.

Apart from the answers collected from the ICT security representatives from the four participating HEIs through interviews (qualitative method); a question was also asked to end users from the three HEIs (HEI01, HEI02, and HEI03) to determine if they have been formally trained on ICT security. The comparison of data from the three HEIs is reflected in cross tabulation Table 6.15 and Chi-Square Table 6.16.

Table 6.11: End users' views on attendance of formal training on IT security at their institution? * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			
			HEI01	HEI02	HEI03	Total
Have you attended a formal training on IT security at this institution?	No	Count	141	144	69	354
		% within Higher Education Institution (HEI) Reference	91.6%	90.0%	97.2%	91.9%
		% of Total	36.6%	37.4%	17.9%	91.9%
	Yes	Count	13	16	2	31
		% within Higher Education Institution (HEI) Reference	8.4%	10.0%	2.8%	8.1%
		% of Total	3.4%	4.2%	0.5%	8.1%
Total		Count	154	160	71	385
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%
		% of Total	40.0%	41.6%	18.4%	100.0%

Table 6.12: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.480[a]	2	.176
Likelihood Ratio	4.238	2	.120
N of Valid Cases	385		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 5.72.

From the analysis of data collected from end users, either been trained on IS security or not (Table 6.15), it can be observed that there were a total of 385 cases of data collected with no missing case. In terms of percentages of their responses, it is evident that almost all the participants from each participating HEIs (HEI01= 91,6% , HEI02=90%, and HEI=97,2% which is an average of about 92%) affirmed to not have received formal training on ICT security at their institutions. A total average of about 8% or 31 participants affirm to have been trained formally in IS security at their HEI.

Further analysis of the responses from the three participating HEIs can be conducted using the Chi-Square Tests (Table 6.16 – Pearson Chi-Square) to determine actual difference in answers from the participants regarding the expectation that the number of participants from the three participating HEIs is equal as opposed to the actual deviations. The results in Table 6.16 reveal also that there is a degree of freedom (df) of 2 with a value of 3.480 or ($X2=3.480$, $df = 2$, and $p = 0.176$ which means $p > 0.05$). Because the p value is greater than 0.05, it can be said that there is no significant difference in ICT security training and the HEIs from which the participant comes from. In other words, neither the origin of the participant (being it HEI01, HEI02, or HEI03), nor the institution itself has influenced the IS security training.

Table 6.13: Place of IT security training * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			
			HEI01	HEI02	HEI03	Total
If yes to the question above, who provided the training to you?	Previous employer	Count	8	2	0	10
		% within Higher Education Institution (HEI) Reference	61.5%	12.5%	0.0%	32.3%
	Own development	Count	5	12	0	17
		% within Higher Education Institution (HEI) Reference	38.5%	75.0%	0.0%	54.8%
	Other	Count	0	2	2	4
		% within Higher Education Institution (HEI) Reference	0.0%	12.5%	100.0%	12.9%
Total		Count	13	16	2	31
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

Further analysis of those who have been trained in IT security (Table 6.16 – about 8% or 31 participants out of 385 who participated) reveals that none of them was trained by their respective institutions. In fact they said that they were trained at:

- Previous employer = 10 participants or 2.6% of total participants.
- Own development = 17 participants or 4.4% of total participants.
- Other reason = 4 participants or 1% of total participants.

The statistics in Table 6.17 on IT security training means that 100% of the participants confirmed that they never received any formal training on IS security from their respective HEIs that participated in this research.

The practice of not providing ICT security training contradicts the best practices recommended by the authors who wrote on the ICT security and importance of end users training. Among the authors are Whitman & Mattord (2014:148) who stated that the only way to enforce IT security in the organisation is when the organisation can prove that it has reached the end users. Thomson & von Solms (2006) also assert that besides the existence and implementation of the security controls such as antivirus, firewalls, intrusion detection systems, the end users are still the greatest vulnerability against the protection of IS resources.

Therefore, many companies offer employees security training to help mitigate breaches. A great concern exist about the possibility of compromise and loss of proprietary information which have reached critical levels in many organisations as a result of staff shortfalls and shortcomings (Kouns & Minoli, 2010:3). Additionally, the lack of ICT security e-competencies has been singled out as one of the issues facing organisations in their quest for the protection of valuable ICT resources (Thomson et *al*., 2006).

The **Question 3** in this section asked the participants through the interviews to share their views on the **challenges** they experience in their respective institutions as the reasons for not training their end users on ICT security. This question also explored other general security challenges that may have a direct or indirect impact on the development of IS security e-competencies.

Through the viewpoint of Activity Theory, this question focused on the challenges the HEIs experience in relation to the tools that need to be associated with the achievement of the object or purpose of the IS security e-competencies development. Also, further focus was given to the willingness of the institutions' community to participate to the activity, and the division of labour among the providers.

This question was only answered through the interviews. The following themes were collected by analysing the participants' opinions:

- Lack of resources, limited budget, and shortage in human resources.
- Struggle with the executives if they do not understand the importance of the assets that you are trying to secure.
- Some of them look at it like a software solution.
- I do not have resources.
- I have got a position of IS security officer which is not filled for many occasions it was advertised.
- Lack of IS security officer.
- Implementation of proper IS security e-competencies development programme not just a piecemeal.
- What will you do when a person is reported? Is the person going to be disciplined?
- You have to integrate difference role players.
- Change of contract to cater for high operating and the performance.
- Ensure that people take responsibility for their actions, based on that you can discipline people.
- People challenge as they do not read the policy and communications.
- People opening an e-mail that has got a virus attachment to it.
- Failure of management to not get involved in the security activities such as disaster recovery management.
- Failure to initiate or build a security culture.
- I wish I had more money to appoint the security personnel.
- The non-separation of duties for system administrator who has got access to end users information is due to lack of resources as they cannot afford more people.
- Lack of monitoring across the systems, because each system has its own tools as we do not have any single tool that covers everything.
- Monitoring is going to be a big issue and we do not have resources for it.
- Not having IS security officer which is a considerable weakness if you do not have one person who is fully responsible for that every day then you tend to manage from incident to incident.

- It is difficult to get the institution to understand especially at universities, if you talk about IT in a company you usually talk to the CIO, universities do not have to have CIOs.
- IT which is seen as a technical function.
- I think it is a major problem for universities and it is getting worse and worse because we now need to comply with these legislations.
- Lack of management commitment to coordinate IT systematically, the IS security and IS security e-competencies development.

The above challenges can be traced to the quotations and views from the participants presented in Appendix F.

From the challenges mentioned, it can be said that each of the four participating HEIs experiences challenges that have a direct or indirect effect on why the IS security e-competencies development programme is not implemented or will not work properly if it is implemented. In general, challenges that are found in each of the participating HEI such as the lack of resources, limited budget, not being able to attract an information officer to coordinate the IS security and training activities, battling for managerial engagement to realise the importance of IS security and its effect on the proper implementation and running of IS security e-competencies development programme.

In relation to the negative effect of limited or lack of resources such as budget for the IS security training programme, Tsohou et *al*. (2012) state that globally, the security training and awareness programmes are either not operating well or investments for the programmes are inadequate. In addition, executive management and boards (university's council) need to consider that the development of IS security e-competencies should also be an activity in the HEI at strategic, tactical, and operational levels (von Solms et *al*., 2011; Ungureanu, 2013). In this regards, the board of the organisation (council) should discuss its importance through their council strategic directives. It should also be included in the security policy and provide support for implementation. In addition, Whitman & Mattord (2010:200)

clarify that "*security training and awareness activities can be undermined if the management does not set a good example and support the programme"*.

Question 4 reads: Which major ICT security threats are you facing in the HEI environment that affects your ICT resources and how do you address them? The question was prearranged on the assumption that the participating HEIs were not training end users on IS security to strengthen their ICT security practices.

From the outset of the answers collected from the participants, the HEIs face both internal and external threats. The internal threats which had 29 frequencies compared to the six frequencies for external threats were more challenging than the external threats. All the four legal services representatives from the four HEIs who participated to this research (**LEG1, LEG2, LEG3,** and **LEG4**) confirmed that internal people with inadequate training on information security are considered to be a potential threat.

Apart from the insiders' threats to IS resources presented in Chapter Two (section 2.3.1.1) of Sakar (2010), Rainer & Cegielski (2013:86-87), the following themes relate to the threats that the four participating HEIs face:

- Internal people make public sensitive research information.
- Internal users level distraction and down time in productivity due to viruses and malware attacks.
- There could be embarrassment when ICT system down time, possibility of hacking into social media account that can expose the institution.
- Abuse of IS resources which did not happen 20 or 30 year ago.
- People not taking responsibility for their IS resources that can lead to complacency and allowing viruses to attack the network.
- Fear of exam paper being compromised because they are on the network.
- Having end users who might not identify that this is a security threat.
- We have been affected by the denial of hard drive access attack which did not come necessarily through the firewall because it could be from USB from home.

- Damage the reputation of the institution is the sending of acceptance letter to all the students who were declined.
- Lack of resources to handle the threats is a threat because there is a responsibility for ICT to play a role in making sure that security is properly communicated and security policy is implemented.
- Stealing someone else account and transferred money into his own account.
- Disclose information related to the tender.
- Altering information like students marks.
- Not complying with Act such as credit Act because of old technology.
- Students can take the institution to court for non-execution of the policy.
- Having end users who cannot know and identify the threats.
- Sending or forwarding of confidential information through e-mail.
- Breaching the confidentiality of information by uploading sensitive information on public network.
- Not keeping track of published researches that can be need for reference.
- Scandals about fake degrees and that can put the institution under reputation damage.
- Issuing of a degree to undeserving student is a threats that you cannot be forgiven.
- In terms of reputation the most damaging ones are those that are not IS security related.

The reference to these themes can be traced to the quotes and views of participants presented in Appendix G.

Still on the question of threats identification, a question was addressed to the end users through the research questionnaire to identify the different security threats that can affect the IT resources they access in their environment. The summary of the responses is presented in frequencies Table 6.18, statistics cross tabulation 6.19 and the Chi-Square table 6.20.

Table 6.14: Frequency table: End users' ability to identify different security threats affecting IT resources they have accessed in their environment

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	125	32.5	32.6	32.6
	Disagree	100	26.0	26.1	58.7
	I do not Know	83	21.6	21.7	80.4
	Agree	56	14.5	14.6	95.0
	Strongly agree	19	4.9	5.0	100.0
	Total	383	99.5	100.0	
Missing	System	2	.5		
Total		385	100.0		

From the frequencies Table 6.18, it can be observed that out of 385 participants, only two participants (or 0.5%) did not complete the question; and out of 383 participants who completed the question, 308 participants or about 80.4% will not be able to identify the threats facing the IT resources they access in their environment.

Table 6.15: End users' ability to identify different security threats affecting IT resources they have accessed in their environment * Higher Education Institution (HEI) Reference Cross tabulation.

			Higher Education Institution (HEI) Reference			Total
			HEI01	HEI02	HEI03	
I can identify different security threats affecting IT resources I have access in my environment	Strongly disagree	Count	52	52	21	125
		% within Higher Education Institution (HEI) Reference	33.8%	32.5%	30.4%	32.6%
	Disagree	Count	35	48	17	100
		% within Higher Education Institution (HEI) Reference	22.7%	30.0%	24.6%	26.1%
	I do not Know	Count	31	38	14	83
		% within Higher Education Institution (HEI) Reference	20.1%	23.8%	20.3%	21.7%
	Agree	Count	25	16	15	56
		% within Higher Education Institution (HEI) Reference	16.2%	10.0%	21.7%	14.6%
	Strongly agree	Count	11	6	2	19
		% within Higher Education Institution (HEI) Reference	7.1%	3.8%	2.9%	5.0%
Total		Count	154	160	69	383
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

Table 6.16: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.916[a]	8	.271
Likelihood Ratio	9.843	8	.276
N of Valid Cases	383		

a. 1 cell (6.7%) has expected count less than 5. The minimum expected count is 3.42.

The cross tabulation Table 6.19 and Chi-Square Table 6.20, present the same trend as observed in frequencies Table 6.16. However, the Chi-Square tests Table 6.18 shows the degree of freedom (df) of 8 with value of 9.916 or (X2=9.916, df = 8, and p = 0.271 which means p > 0.05). Because the significance is greater than 0.05, it can be concluded that there was no significant difference in the answers provided by the participants on the ability to identify the threat facing the IT resources they access in their environment and the HEI they are affiliated with.

The results in Table 6.20 confirm participant SEP01 from HEI01 allegation "*they might not know that it is a security threat and they might not identify it*" when posed with the question if end users know what to do in case of security threats In this regard, end users become a permanent threat to ICT security.

To control the internal threats, the participants of interviews agreed that the way to deal with internal threats is through security training, awareness, and proper procedures and enforced security policy. From the data analysed, the four participating HEIs have not implemented these measures fully as training and awareness, and even the enforcement of security policy are still far from full implementation.

The above measures for dealing with internal threats as participants suggested link with the best practices of authors who wrote on the issues related to personnel security. Among them Ettinger (1993) identifies procedures and practices such as

screening, security clearances, supervision, and training and awareness on IS security as the most related issues. Piccoli (2012:395) suggests measures to emphasise security policy which articulates the behaviour of staff and separation of IS resources that are made available to different category of employees. Humphreys (2007) mentions, among other measures, the reading, understanding, and signing of security documents and related sanctions, provision of training and awareness appropriate to employment, and also the immediate implementation of the working leave for highly privileged employees.

After dealing with internal threats, these paragraphs present the reported external threats that IS resources face in the HEIs and how they are dealt with. Apart from the list of the external threats that affect general ICT resources in organisations as discussed in Chapter Two (Section 2.3.1.2), the participants from the four HEIs highlighted the external threats such as the denial of service attacks, the network hacking, stealing of ICT resources in areas with no management.

The external threats according to the summary of answers collected from the participants, that are dealt with through the use of ICT security technologies include intrusion prevention systems, firewall, and network controls. These relate to the external threats that are presented in the literature review by Okenyi & Owens (2007), Rhee et *al*. (2009), Furnell (2009), Brehm & Gomez (2010), and Harwood (2011:104-120), Piccoli (2012:395-398) and Rainer & Cegielski (2013:94-103). These authors include actions such as access control, cryptography, creating backups, and security hardware and software.

Apart from the application of the technology to protect against external threats and use of security policies and procedures to deal with the internal threats, the current practices used to protect ICT resources in the participating four HEIs that were repeatedly mentioned include the installed antiviruses on their systems, the use of vulnerability management systems that scans their network infrastructure, ensuring that proper role-based access control is granted to appropriate end users with regular monitoring, and ensuring that external auditors assess the strength of their ICT infrastructures and recommend necessary actions for improving weak links.

From this section, the security experts from the participating HEIs and those from other HEIs recommended that:

- For the new staff members coming on board, as part of induction, everyone must be trained and made aware of IS security and this must be compulsory (participants from institution **HEI01** – **SEP01** and **SEP02**).
- The change in behaviour such as not taking the memory sticks used by students that might be infected by viruses (**EXP07**) and the use of user education and appropriate technologies such as IDS, spam filtering, and firewall (**EXP10**) to proactively act against internal and external threats.

Apart from the benefits derived from the training of employees in general and in particular in ICT security, the implementation of training and awareness programmes globally are either not sufficient, or the investments in the programme are inadequate. The latter reflects the challenge that all the participating HEIs are facing. All HEIs lack the necessary budget to attract an IS security officer who can coordinate the security activities in the institutions. In fact, almost all the interviewees mentioned that their budget was either not sufficient or they cannot quantify the level of budget allocated to ICT security activities.

Apart from the budget challenge, another challenge that makes staff members to be disinterested in IS security e-competencies development is the failure to provide the specific aspects of training that matters for employees according to their jobs and how these aspects relate to the employees' work environment and operation. This challenge has been identified and solved in this research through the identification of key end users of IS resources in the HEIs. Also determined, was their levels of responsibilities in order to identify the appropriate level of IS security training to match their job.

Question 5 required the participants to rate their institution commitment to the development of IS security e-competencies given the practices they have described.

In reference to the Activity Theory (AT), this question related to the achievement of the object or purpose of the activity system. Of interest is that the participants rated

the commitment of their institutions less than 3 out of 5. In particular they said the following:

- From **HEI01**, participants **SEP01** and **SEP02** agreed that "*on the development of IS security competencies among the end users the institution is at the beginning*".
- From **HEI02**, participant **SEP03** said that "*we are very far away from what we want to do, we have got things in place that add value from the system point of view but not from users point of view*. *You cannot get into the system without getting through approval process it is not easy, so the element that we have put in place is to control things, so the end user does not need to know everything*".
- From **HEI03**, participant **SEP04** also stated that "*there is always room for improvement, we understand security, but understanding your security landscape is difficult and that is where we lack a bit*". "*We need to understand our landscape more, always enabling people to do their job. I think we can run more IS security awareness campaign"*.
- From **HEI04**, participant **SEP05** said that there "*is the intent to develop end users IS security competencies, but there is no sufficient commitment*". "*The question of not always balancing resources and the risks and the general philosophy of us to delegate and distribute the responsibility rather than to have a single person responsible throughout the university, I would like to see a stronger commitment, and that is a weakness"*.

The low rating of participants from the four participating HEIs shows that these institutions have concentrated the IS security effort more on ICT technologies. Thus, the impact of IS security e-competencies development in the ICT security programme have been underestimated. In this case, it is difficult for the ICT departments from these institutions with their depleted budget and resource challenges to address the IS security training if there is no management direction and support.

The authors who have written on the IS security in general and training in particular have suggested that effective security training and awareness programmes need to

be enforced by senior executives through their security policy (Henry, 2004 as cited in Thomson & von Solms, 2006). Also, it is essential that behaviour be modelled according to the security culture. Chapman et *al*. (2010) confirm that "*management involvement and accountability can greatly influence the employees' behaviour*".

6.3.2.3 Sub-objective 3: The exploration of optimal ways of supplying the needed IS security e-competencies in the HE environment

The previous section discussed the importance of IS security e-competencies development and the current practices of IS security e-competencies development from both IS security experts. Also, the point of view of the management as the registrars' offices hold, and the end users from the four participating HEIs believe, was described. This section focuses on how the IS security e-competencies can be supplied to the end users in the HE environment.

In relation to the Activity Theory (AT), the questions in this sub-objective related to the subjects in the activity system in terms of those whose needs for IS security e-competencies development has to be analysed, the suppliers or the training whose capacity needs to be analysed, and to ensure that proper division of labour and the necessary tools are available to achieve the object of the activity system.

For this section, questions were also asked to participants using interviews and the questionnaires as discussed below.

Question 1 read as follows: Who are the key end users (subjects) of IS resources and how can they be classified in terms of their responsibilities and needs for IS security e-competencies? This question was asked to identify the key end users and their need for security e-competencies to be able to categorise them in the final framework of this research.

The following themes were compiled from the interviews with the participants:

- Everyone who is using ICT resources is a key end user.
- The end users can be categorised in students, the staff, and the super users who deal with the application of policies, and the system administrators.

- The data managers who do not need to have access, but authorise access.
- The system administrators because they have got access to almost everything, and then the developers.
- We have three types of end users: first group is made of administration, then teaching and learning users, and the end users in research department.
- We rely heavily on the concept of information curator, their responsibility and accountability.
- The curator of information, for instance in HR division the head of HR.

These themes were identified from the participants' views during the interviews and are linked to the participants as presented in Appendix L.

It is clear that for each institution there is a person in charge of the department such as the HR director, finance director, or any other director who for the purpose of consistency is called department information curator. This person is in charge of setting operational procedures and authorise access to information. Then there are information officers who implement the decision for data access. In the third instance, there are departmental officers who authorise special requests like large amount of procurement and financial transactions. From the discussion on the access, it is acknowledged that being highly ranked in the HEI like vice chancellor or IT director does not mean that you will have access to everything. Only system administrators have access to most of the data. In fact directors do not need to have access to all data. In most cases directors access the system through their assistants or they get information from their subordinates.

The understanding and recognition of levels of end users is an important aspect of IS security e-competencies development and the development of IS security e-competencies framework for the end users department. This will assist in identifying additional security e-competencies that end users need when promoted from one position to another (Schulz et *al*., 2013). It is also important to tailor IS security training according to the skills levels of employees (Morelock, 2012; Sedinić et *al*., 2014) as the end users can been given new tasks to perform at the require additional

level of IS security e-competencies, which could be different from those of the previous position.

Question 2 states: What is the importance of IS security e-competencies development for the end users and the institution? This question was asked to both the interview participants and the end users to determine if they value the importance of IS security e-competencies with regard to the operations of their institutions and their activities.

From the interviews with participants from the four HEIs, they all believe that the development of IS security is an important part of security measure because of various reasons. Most importantly it is related to the following themes:

- Compliance with the new laws such as POPI.
- To educate end users on how to handle information and before applying any disciplinary measures for mishandling the information.
- End users are part of ICT security programme.
- End users have the responsibility to protect their access details and log off properly from the critical IS resources they use.
- End users need to manage their data and systems of their departments.

The same question was also asked to the end users from the participating HEIs and the summary of answers is provided in the Tables 6.22 and 6.23).

Table 6.17: Frequency table: the relevancy of the IT security competencies towards the end users' work

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Additional work	30	7.8	7.9	7.9
	Important for me and IT resources	266	69.1	70.2	78.1
	Irrelevant to me	42	10.9	11.1	89.2
	No choice	41	10.6	10.8	100.0
	Total	379	98.4	100.0	
Missing	System	6	1.6		
Total		385	100.0		

Table 6.18: Statistics - the relevancy of the IT security competencies towards the end users' work

N	Valid	379
	Missing	6
Mode		2

From the frequencies Table 6.22 and from the statistics Table 6.23, it can be observed that out of 385 participants, 379 participants (about 98.44%) successfully answered the question and only 6 participants (about 1.56%) did not answer the question. From those who answered the question, the majority of participants (70.2%) affirmed that IT security competencies are important for them and the IT resources they access. This is also confirmed in the statistics Table 6.23 as the Mode = 2 (important for me and IT resources).

Table 6.19: The relevancy of the IT security competencies towards the end users' work * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			Total
			HEI01	HEI02	HEI03	
How relevant are the IT security competencies in relation to your work?	Additional work	Count	13	5	12	30
		% within Higher Education Institution (HEI) Reference	8.6%	3.2%	17.4%	7.9%
	Important for me and IT resources	Count	104	124	38	266
		% within Higher Education Institution (HEI) Reference	68.4%	78.5%	55.1%	70.2%
	Irrelevant to me	Count	17	14	11	42
		% within Higher Education Institution (HEI) Reference	11.2%	8.9%	15.9%	11.1%
	No choice	Count	18	15	8	41
		% within Higher Education Institution (HEI) Reference	11.8%	9.5%	11.6%	10.8%
Total		Count	152	158	69	379
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

Table 6.20: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	18.890[a]	6	.004
Likelihood Ratio	18.220	6	.006
N of Valid Cases	379		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 5.46.

The cross tabulation Table 6.24 demonstrates that the higher percentages of end users (266 participants or 70.2%) concur to the answers collected from the interviews in terms of IS security competencies' importance to them and the IT resources they access.

The Chi-Square test (Table 6.25) was also used to test how significant the difference is of the participants' answers on the relevance of the IT security competencies in relation to their work and their HEI. The values received were: df = 6 with X2=18.890, df = 6, and p = 0.004 which means $p < 0.05$. Because the p value is less than 0.05, it is concluded that a significant difference exist on participants' answers on the relevance of the IT security competencies in relation to their work.

The difference is due to the fact that from HEI01 68.4% agreed to the importance, from HEI02 78.5% agreed to the importance, while from HEI03 55.1% agreed to the importance. In general, the total number of those participants who agreed that the IT security competencies were important for them and the IT resources they access was higher than those who disagreed even though the percentages were not the same.

Question 3 states: What are the challenges you experience when you train staff members in the institution? This question was answered from the interviews mainly with the training and development department to highlight the challenges in general

training and development. Furthermore, it was to show how the challenges can affect the development of IS security e-competencies.

As it was with the challenges in the development of IS security e-competencies, this question asked for the challenges related to general training and development. It was linked to tools, rules, the subjects, and the division of labour among the participants in the achievement of the object of the activity system.

From the interviews with the participants, the following themes were recorded in relation to this question:

- Most of the training sessions are offered on the main campus, there is a need to identify other means of delivering training such as online.
- There are also challenges related to limited budget.
- The scheduling of training to accommodate conflicting schedules of academics and administration and support staff.
- Cancellation of training by the staff members after the registration.
- People want to come to training but they have much work and the workload.
- People come to the training but they have got the attitude of what is the point of coming.
- Staff complement, and the dispersion of training budget to individual department which the central training and development cannot control.
- Organising training when you have got so many campuses is a challenge in that most of the trainings take place at main campus.
- When the staffs need the training they have to travel.
- Limited budget for training as there has been budget cut for the last three years.
- Management of the relevancy of the skills such as matching the right programme to the right skill, and getting the right group in the classroom.
- Limited budget as the biggest challenge.

The above challenges are linked to the views and quotations from the participants as presented in Appendix M table.

From these challenges, the budget and shortage of staff members could impact the development of IS security e-competencies if management provide no additional support. With reference to previous research, Tsohou et *al*. (2012) confirm that globally security training and awareness programmes are not operating as it should be and/or investments are inadequate.

Question 4: If you were asked to develop (train) end users in IS security e-competencies, what could be the content of your training? This question was asked to the ICT experts from the four participating HEIs to discover the content of IS security training programme if it is to be provided.

In relation to Activity Theory, this question was linked to the analysis of tools needed for the training and the division of labour among the participants to the activity system.

The general perspective and common themes related to training content derived from participants answers varied between basic understanding of security technologies and environment (internal and external) to the procedures and processes such as those related to login and password selection and protection. However, it also included to make people aware of the implications of data and other IS resources mishandling such legal implications and related disciplinary process.

In particular, the participants mentioned the following contents to which are added those themes that experts from other seven South African HEIs mentioned. These are presented in Appendix E. The following themes were compiled in relation to this question:

- Taking ownership of your responsibilities.
- Proper management of user environment by taking care of your access details and IS resources as you would take care of you bank ATM card.
- Not disclose where they must not disclose.
- Proper login and log off.
- End users are responsible of the consequences if they do not log off.
- Inform them also of the risks and the threats.

- Inform them on the procedures such as who contact in case of threat (possibly give contact number).
- Emphasis on good practices and to make people aware of the risks if good practices are not followed.
- Train them on risk of viruses.
- Focus of the awareness as who has got access to information, whom has got what right, when they have got access to your information.
- What mechanisms they use to gain access and to exercise their right.
- Tight control of user name and password.
- They need to understand what the risks are when protecting those user names and passwords.
- Inclusion of legal requirements and Acts such as the Promotion of Access to Information (PAI) act, Electronic and Communication Transaction (ECT) act, and the Protection of Personal Information (POPI).

In relation to the legal requirements, the participants also agree that the institution is liable for any legal requirement breach as it is now with POPI. However, more focus is needed as the risks have been more defined and there are specific penalties in case of non-compliance. For these reasons, HEIs need to ensure that end users are trained and understand the disciplinary requirements related to the breach of legal requirement.

In relation to the question on the importance of the knowledge of legal requirements for the protection of IS resources, the end users were also asked a question in the research questionnaires to determine if they understand the implications of legal requirements for the protection of IT resources they access. From the summary of research questionnaires collected it was generally established that the knowledge of legal requirements in the protection of IS resources was also deemed important. Participants' answers are established in Tables 6.25 to 6.27 produced by SPSS software for quantitative data analysis.

Table 6.21: Statistics – End users' knowledge of the legal implications of their actions on IT resources and related security

N	Valid	383
	Missing	2
Mode		1

Table 6.22: Frequencies – End users' knowledge of the legal implications of their actions on IT resources and related security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	118	30.6	30.8	30.8
	Disagree	88	22.9	23.0	53.8
	I do not Know	104	27.0	27.2	80.9
	Agree	41	10.6	10.7	91.6
	Strongly agree	32	8.3	8.4	100.0
	Total	383	99.5	100.0	
Missing	System	2	.5		
Total		385	100.0		

From the statistics Table 6.27 and frequencies Table 6.28 it is evident that out of 385 participants who received the questionnaire 383 participants (or 99.5%) completed the question while only 2 participants or 0.5% did not answer the question. From the 383 who answered the question, the majority of them (a cumulative percentage of 80.9%) acknowledged that they either do not know (27.2%), disagree with the question (53.8%), or totally disagree (30.8%) with the question that they know the legal implications of their actions on IT resources and their related security. It can also be observed from the statistics Table 6.27 that the class modal or most recurring answer was 1 (strongly disagree).

Table 6.23: End users' knowledge of the legal implications of their actions on IT resources and related security * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			Total
			HEI01	HEI02	HEI03	
I know the legal implications of my actions on IT resources and related security	Strongly disagree	Count	51	46	21	118
		% within Higher Education Institution (HEI) Reference	33.1%	28.7%	30.4%	30.8%
	Disagree	Count	35	35	18	88
		% within Higher Education Institution (HEI) Reference	22.7%	21.9%	26.1%	23.0%
	I do not Know	Count	30	54	20	104
		% within Higher Education Institution (HEI) Reference	19.5%	33.8%	29.0%	27.2%
	Agree	Count	16	18	7	41
		% within Higher Education Institution (HEI) Reference	10.4%	11.3%	10.1%	10.7%
	Strongly agree	Count	22	7	3	32
		% within Higher Education Institution (HEI) Reference	14.3%	4.4%	4.3%	8.4%
Total		Count	154	160	69	383
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%

The cross tabulation Table 6.29 describes the same trend of the majority of end users (a cumulative percentage of about 81%) that either do not know, disagree, or

totally disagree that they know the implications of legal requirements on the IS resources they use.

Table 6.24: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	17.779[a]	8	.023
Likelihood Ratio	17.729	8	.023
N of Valid Cases	383		

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 5.77.

The Chi-Square test reveals (Table 6.30) the degree of freedom (df) of 8, X2=17.779, df = 8, and p = 0.023, which means p > 0.05. Because the significance is greater than 0.05, it can be concluded that there was no significant difference in the answers of participants on their knowledge of the legal implications of their actions on IT resources and related security and the HEI they belong to. In other words, although the employee are coming from HEI01, HEI02, or HEI03, the majority of them would still not know, disagree, or strongly disagree to the question that they know the legal requirements related to the IT resources they use and their related security.

In relation to this research, legal requirements ensure that organisations that collect and process personal information of their stakeholders (automated and non-automated intended to form part of filing system) fulfil the obligation to ensure that the collected information are protected against any disclosure for other purpose than it was collected for. Additionally, the legal regulations combat against the rise in the abuse, misappropriation, and unintended use from the part of the authorised users and unauthorised criminals who access the IS resources illegally to collect the data (information) for illegal activities, to cause panic, provoke catastrophe, and financial gains (Ciampa, 2014:18; Yoon & Kim, 2013; Bhargav & Kumar, 2011:20). Thus, the

legal requirements and Acts that address IS resources security include POPI, PAI, and ECT and need to be part of the content of security training.

The content of training as participants presented, are also in line with the suggestions of Smith (2009) to include the human factors, and errors. Also, Rhee et *al*. (2009) presented important issues like writing down password, sharing password, and also employees' carelessness with mobile IS resources such as laptops.

Question 5 narrates: What are the current practices and approaches to training that have been adopted by your department and the institution? This question was asked to discover the current training practices and how they can impact the development of IS security e-competencies in the institutions.

In relation to the Activity Theory, this question was asked in order to analyse the current tools used in the delivery of training. Furthermore, it explored the impact on the delivery of effective training in the current moment, and to which extent they can support the IS security e-competencies development.

As discussed in the previous section, the four participating HEIs do not formally train end users on the IS security. Neither does any formal discussion takes place on IS security, except the provision of limited information during other training on MS office SAP. Most IS security related information is provided in the form of newsletters and documents that are uploaded online which intended end users do not usually read.

The following themes were collected during the interviews with the participants from the four HEIs regarding approaches to training:

- Through newsletters and information sessions we try to make users aware of risks of viruses.
- We run awareness campaigns like do not open mail if it has got .exe file in it.
- We say in our e-mails that go from the help desk we will never ask you your user name and password.
- The awareness is provided through newsletters and publications.

- Through information sessions with the IT staff, if it is the rest of the university it is through newsletters and electronic publications and emails.
- The training is open to all staff members (permanent and on contract).
- Induction programme is used to introduce the newly appointed staff members to the operation of their respective institutions.
- The participation to all training sessions is not compulsory.

These themes can be traced to the participants' views and quotations presented in Appendix N table.

The current practices on IS security e-competencies development moves more toward informing end users about ICT security threats through e-mails, news groups, and publications rather than training for hands-on experience on how to deal with the threats. These methods are seen as supporting method to training. In most cases end users would not be able to understand the content of the message or they barely read the e-mails and other communications. This weakness calls for the participating HEIs to find ways to train employees before implementing supportive methods such as newsletters and e-mails.

The reviewed literature also asserts that there is a need to move from the informative newsletters and e-mails to more practical training to inform end users how to deal with the threats that are continuously changing (Rezgui & Marks (2009). This implies that the training supplied to end users has to also ensure that the end users' behaviours change (Rhee et *al*., 2009) to be in line with the changing threats.

Question 6: Which methods do you use to provide training to the employees in your institution and how effective are they in meeting the current needs and those of IS security e-competencies development? This question was asked to identify the appropriate method (s) of supplying end users security e-competencies. It relates to the tools intermediating between the subjects who are the recipients and the subjects who are the suppliers of training in the achievement of the object of the activity system.

From the responses of the training and development representatives from the four participating HEIs, the common theme that emerged was the use of classroom method (contact mode) as the main method for training. Regarding method, the HEI03 mentioned the use of the online method for certain practical subjects like project management that require students to do exercises and submit them.

The reason for selecting classroom method is that the learners have the opportunity to learn from one another, and ask questions. Despite the advantages of the classroom method, participants also expressed a much known challenge, namely its limitation to attract participants who are situated at different campuses. There are also those people who will not be able to attend training when the classroom method applies, for various reasons. Therefore, another method needs to be added to the preferred choice. An alternative for attending additional training after the formal classroom training during the induction should be offered.

Beisse (2013:479-519), and Salas et *al*. (2009) who have written on the topic of training propose other options (methods) that can be associated to the classroom method such as reading assignments, online reading assignments, hand outs and reference sheets, role playing, collaborative or group learning, computer-based training (CBT) and Web-based training (WBT).

In addition to the use of the common classroom method, there was also agreement amongst the participants on the following aspects of training:

- Participants accepted the idea that an awareness campaign be run as an online scenario with questions that end users have to answer at the beginning of each year before entering into any other work on their computers. Employees will have a number of days to complete the exercise, after which the access to services will be cut. This method was successfully run at Interior (Robinson, 2006). Even though the participants did not say that the yearly activity could fully solve the problem, they suggested that it can help the process.
- HEI04 SEP06 believed that the induction mechanism is a very good mechanism and part of the implementation of POPI. For instance, the

awareness plan can involve things like making sure that activities (training on IS security) are included in the induction programme.

- The participant SEP03 from HEI02 also referred to practices in other corporations like running competitions. "*We can track how complex your password is, and you give somebody who gives a very strong password a prize"*. Other quotes included: "*Culture based on these types of things you must do it quite happily. Have you checked to see whether your password changes properly? Have you changed your laptop password? These are the types of things you can put into the equation and get people involved; if you do not get people involved forget about it"*.

Both literature on the security training and awareness and the interviewees of this study distinguish between awareness and training. EXP14 said that "*awareness is very much seen as a reminder, but a reminder of what if the participating HEIs never provided formal security training*"? In fact Whitman & Mattord (2010:193) confirm that security training "involves the provision of detailed information and hand-on instruction to end users so that they can perform their tasks securely".

This research agrees to the proposition that security training should precede the awareness campaign. It is important as it acts as alerting the already trained staff members on the new development related to ICT security threats, controls, and procedures since the previous training during induction. Both training and awareness contribute to the security of information and IS resources that process them. Eminağaoğlu et *al*. (2009) mention that an awareness campaign is added to training courses to complement the training as employees may forget the content they were exposed to during the training. Finally, Humphreys (2008) states that IS security awareness is part of good business practice. Education, training, and awareness are part of organisational education programmes intended to reduce security breaches resulting from employee ignorance and lack of awareness (Zafar, 2013).

The participants acknowledged that the selection of one particular training method does not necessarily mean that it is better than others. It only stresses that it accommodate the need of the particular group. It also addresses the training

objective as each training method has its advantages and disadvantages (Beisse, 2013:495). However, from the available options, the Internet-based option is the recommended option for training. This is the most cost-effective method and has the possibility for reaching the majority employees compared to face-to-face initiatives which is more resource intensive (Ruzek, et *al*., 2012). It could also help in reaching even those employees dispersed across other campuses and sites who want to attend the training but could not leave their desks for various reasons.

To conclude this question on training methods for the supply of IS resources e-competencies to the end users; two questions were added for completion through the research questionnaires. The first question asked whether the participants would attend the IS security e-competencies development training if it is provided by the institution. Secondly, the end users were asked about which training method they prefer if to choose between the contact modes, online mode, training materials provided on CD or DVD, or material printed for self-reading. The following three tables (Table 6.32, Table 6.33, and Tale 6.34) summarise the answers collected from the end users. It also outline whether participants would attend the IS security training or not.

Table 6.25: End users' willingness to attend institutional IT security training related to their job level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	52	13.5	13.5	13.5
	Yes	333	86.5	86.5	100.0
	Total	385	100.0	100.0	

From the frequencies Table 6.32 it is evident that from all the participants who completed the questionnaires all of them (385 participants) answered this question and the majority of them (333 or 86.5%) said that they would attend the training as compared to 52 participants (or 13.5%) who said that they would not attend the training.

Table 6.26: End users' willingness to attend institutional IT security training related to their job level * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			Total
			HEI01	HEI02	HEI03	
Would you attend institutional IT security training related to your job level?	No	Count	17	16	19	52
		% within Higher Education Institution (HEI) Reference	11.0%	10.0%	26.8%	13.5%
		% of Total	4.4%	4.2%	4.9%	13.5%
	Yes	Count	137	144	52	333
		% within Higher Education Institution (HEI) Reference	89.0%	90.0%	73.2%	86.5%
		% of Total	35.6%	37.4%	13.5%	86.5%
Total		Count	154	160	71	385
		% within Higher Education Institution (HEI) Reference	100.0%	100.0%	100.0%	100.0%
		% of Total	40.0%	41.6%	18.4%	100.0%

Table 6.27: Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.163[a]	2	.001
Likelihood Ratio	11.359	2	.003
N of Valid Cases	385		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.59.

The conclusion that can be drawn from the cross tabulation Table 6.33 is that while the majority of end users (86.5%) confirmed that they would attend the training, most of them would attend from HEI01 and HEI02 which have 89% and 90% respectively. Instead, the HEI03 has 73.2%. Despite the differences in the answers, it can still be observed that all of the participating HEIs have a high percentage of participants who would still attend the training.

From the Chi-Square tests Table 6.34 the perceived value is X2=13.163, df=2, and p= 0.001, which means p<0.05. Due to the fact that the p value is less than 0.05, it can be concluded that there is a significant relationship between the HEI and the acceptance to participate in the training and development. Given the high percentages of the participants from all the three participating HEIs (73.2%, 89%, and 90%) presented in the cross tabulation Table 6.33, it can be said that all of the three participating HEIs can still expect a high attendance during the IS security training.

The second question asked to end users in the questionnaire was to select which training method (s) they prefer from the four methods proposed: contact mode, online mode, training materials provided on CD or DVD, or printed material for self-reading. The answers to this question were analysed per training method in the four frequencies tables (from Table 6.35 to Table 6.38) below.

Table 6.28: End users' preference towards classroom (contact) mode

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	16	4.2	6.8	6.8
	Yes	219	56.9	93.2	100.0
	Total	235	61.0	100.0	
Missing	System	150	39.0		
Total		385	100.0		

Table 6.29: End users' preference towards online training mode

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	26	6.8	16.0	16.0
	Yes	137	35.6	84.0	100.0
	Total	163	42.3	100.0	
Missing	System	222	57.7		
Total		385	100.0		

Table 6.30: End users' preference towards information provided on CD or DVD

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	36	9.4	28.8	28.8
	Yes	89	23.1	71.2	100.0
	Total	125	32.5	100.0	
Missing	System	260	67.5		
Total		385	100.0		

Table 6.31: End users' preference towards printed notes for self-reading?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	30	7.8	20.4	20.4
	Yes	117	30.4	79.6	100.0
	Total	147	38.2	100.0	
Missing	System	238	61.8		
Total		385	100.0		

From the four frequencies tables (Table 6.35, Table 6.36, Table 6.37, and Table 6.38), it is perceived that the majority of end users preferred method of delivering in the following order:

1. Contact mode (56.9%);
2. Online mode (35.6%);
3. Printed notes for self-reading (30.4%); and
4. Lastly the information provided on CD or DVD (23.1%).

The percentages add to a total of more than 100% because participants were required to select more than one method if possible. The participants preferred mostly the contact mode because of its possibility for interaction with the trainer and as it provides opportunity to ask questions and quick feedback, focus during the training, possibility for hands-on activities and is more effective. Likewise, it provides for to interaction with class mates. The disadvantage of the contact mode of training was the time limitation, as it may be in conflict with other work activities.

The second mode of delivery that participants preferred was the online mode. The reasons being that it is flexible or accessible anywhere, enables learning at own pace, convenient and not clashing with lecturers teaching time, and it gives the participants the possibility to do the training at their own time. The disadvantages of the online method that participants mentioned include the interruption when focusing on training, not easy to follow, and no personal contact with the trainer. One participant also mentioned also that the online method can be used as a memory backup for contact mode training.

Even though the printed note for self-reading and the DVDs were less selected than the other two methods, the participants mentioned it as relevant and convenient to allow for the pace of the participant, to be executed at one's own time and can be used for reference after the training. The participants mentioned this method is inclined to be boring, not environmental friendly, and can also be confusing, much troubling and can be potentially lost.

Even though the answers from the interviews suggest that the training method depends on the needs of individual training, the participants' selection allows for the research to recommend the combination of contact as the initial method of training to facilitate the understating among the end users and help them clarify the concepts and other challenges with the trainer. Then the contact mode can be supported with the online mode to remind the participants who attended the training on the development to deal with threats, to reach the participants who could not attend the training due work commitments, and use it also for the training activities at the beginning of each semester before the end users start to work on their computer systems.

Literature that supports the training methods include the writing of Lucas (2012) who recommends a mixture of methods (such as contact and online modes) to accommodate different training styles. Additionally, as in the case of this research a mix of training style will accommodate the employees who could not attend the contact mode due to other works commitments.

In general, it can be said that the content and the supply of the training contribute to the implementation of security policy. This is because the security policy is implemented through the training, awareness, and communication with employees.

6.4.2.2.4 Management and end users' views of IS security in the HE

During the interviews and distribution of research questionnaires, the researcher diarised some views on IS security from participants (management, security experts, and general end users). These views showed IS security and security e-competencies development practices in the four participating HEIs is still at infancy stage or not well cultivated. We start with the presentation of general management views and security experts' views, and then extend to the views of general end users:

- On the decision to train the end users on IS security, the **REG2** from **HEI02** said that "*I do not think that it is the council decision. Council does not manage the university, it is a management issue. It is not governance issue;*

Vice Chancellor and his portfolio managers must ensure that staff members are trained in this particular issue".

- The participant **REG2** continued to say that "*institution has not made much effort to ensure that the staff members really understand the issue of access to information and how to use the information at their disposal and actually how to secure the information that has been provided*".
- On the budget allocated to ICT security activities, all the participants believe that their budget is insufficient, and it is estimated to range from 0.5% according to SEP04, 2% according to SEP05, or "*it is difficult to determine the budget but less than it should be"* according to SEP06 and SEP03. The participants **SEP01** and **SEP02** from **HEI01** said that "*executives do not recognise IT as important; this is why it can be said that the IS security budget estimated of less than 5% is not right*".

From the security experts, the following views were recorded that emphasised that IS security management is still in infancy or not enforced:

- From the **HEI01**, the **SEP01** and **SEP02** said that "*certain security training works well with the individual principles and behaviour, what you can do is to enforce the controls, but it works well in corporate environment as it is against the ethos of the universities to tighten the control or lock down everything. So at the moment our computers are open, there are no policies on them except the antivirus but you can download and install anything*".
- From the **HEI01**, the **SEP01** and **SEP02** mentioned that *"certain lab administrators do not like the antivirus which is provided by the ICT department, they download their own antivirus".* This behaviour shows that there is lack in emphasising control and policies in the HE environment.
- From the **HEI01**, the **SEP01** and **SEP02** continued in that for "*most of the time universities are essentially open, we have in the past believe that there is no threat because information is open, which is increasing fear of identity theft, reputation damage, and now the fact that universities are responsible for generating income out of the research I think that has made us more security aware that we need to start guarding our assets, we need to classify, we need to start guarding our assets*".

- From **HEI03**, the participant **SEP03** made reference to the open ease of access to IS resources and confirmed that *"the password at the institution (**HEI03**) never expires to make the services accessible*".
- Concerning the use of ICT security management frameworks, the respondents from all the participating HEIs said that they do not use the frameworks currently. Specifically the respondent **SEP03** from **HEI03** said that "*we have not managed to use the standards, but we are aware of them, we have not implemented because they are costly, ISO27001 we are not a bank but we use the guidelines, we cannot implement it, you cannot see the bank running a DMZ, you cannot see the bank never changing the password*".
- The participant **SEP06** from **HEI04** mentioned that *"the openness of universities make them different to other business companies. You cannot ban Facebook, we do not monitor what people look at, and if they are look at porn that is their problem. That is the university; there is a certain freedom and openness that must take place and there is also academic independence, so it is a very difficult place to coordinate*".
- From the **HEI04**, the participant **SEP06**, who is the director of IT security and governance stated that "*we have not done any formal IS security training, in any case our senior people I think they understand very well what the risks are, we do not have to tell the registrar that students records are confidential, he knows very well*".
- From the **HEI04**, the participant **SEP06** stated on information security policy that "*we have had information security policy since 2008, the only time that the university takes it seriously is when there is a very specific risk and up to now there has never been specific risk information security, they will say it is important but tell me why, but now with POPI I think it is going to take more focus because the risks as they need to be defined and there are specific penalties for that*".
- On the IS security training for employees the participant **SEP06** said that "*the induction mechanism is a very good mechanism and part of the implementation of our POPI for instance the awareness plan involves things like making sure that activities like that are included in that induction. But again the university is not a bank, I think it security is at totally different level*

at university, my personal view is it could be serious when a security breach could call the integrity of the university qualifications into question, then it becomes serious because that is what the university is, it certifies that the person has this qualification if that ever becomes a question then we got a problem".

- When asked about the usage of ICT management framework in managing IS activities, respondent **SEP06** from **HEI04** declared that "*this aspect is better understood in the industry because I think companies are simpler, the university business is complex, there is teaching and learning, there is research, there is community interaction, dealing with knowledge, and there is also academic independence, so it is a very difficult place to coordinate, you can coordinate the administration of information security but trying to coordinate the academics around the information security that is a different game*".

From the general end users the following views on IS security and security competencies were recorded:

- One participant at the institution (HEI02) said "*I am working for finance department, what I have to do with IT security policy*?"
- Participant 136 responded to the question on the location of security features on the computer: "*I think you refer to the cable at the end of my computer? Security cable*".
- Participant 137 said "*I have no responsibility of IT resources security, but the security of my own documents and information on the computer*".
- Participant CP160 thought "*IT security is not my responsibility, but I create log files for staff all the support in the creditors department at the institution (HEI02)*". This indicated that the participant is the information manager in the user department.
- To demonstrate the technological failure in protecting IS resources against the threats, one participant from HEI02 articulated "*I perceive IT security is end users' responsibility, we run Geographical Information Systems (GIS), we need to be more aware of IS security. Our spam filter is not working, so we receive unwanted e-mails every hour*".

- Participant 65 from HEI01 said "*I cannot remember reading security policy at any time*".
- Respondent CU13 from HEI03 said: "*If it is my technology, the security of IT resources is my responsibility. But if it is their (Institution and its technicians) network, it is their responsibility*".
- Participant CP100 declared that she "*has asked for this IT security training for years and have been silenced*".
- On the knowledge of legal implications, participant 278 displayed "*I am an academic and therefore it is not responsible for that. I assume an IT specialist looks after IT security. I would attend information session*".
- One participant questioned "*Do we have institutional IT security policy? I have never seen it*".

From the point of views of the registrars representing each of the four HEIs, the IS resources are at the centre of administration and delivery of education in the HE environment (from students' registration to the issuing of certificates). This is also the point of view presented in the Post-School education and training Green Paper published by the Department of Higher Education and Training (DHET, 2012). The Green Paper states that IT resources are an important part of participation in the global world and the provision of education at the post-school level. On this level, IT resources have moved from supportive to become enablers of HEIs operations, teaching and learning (Johl et *al*., 2013).

To conclude this chapter, Buecker (2007) confirm that in securing IT is deemed fundamental for any business. In addition, IS security e-competencies development through security awareness and training is considered part of the information security management, though less investment is made into the programme compared to security technologies (Tsohou et *al*., 2012).

One of the contributors that cause IS security e-competencies development to be unsuccessful in the organisation prove to be the ignorance of the information security management team (and possibly the management). Management do not see the inherent variability of humans and their impact on the information security in the

organisation (Frangopoulos, 2007) as Rastogi & von Solms (2012) also mention. Due to a trust deficit, the security manager believe that end users lack skills, motivation, and knowledge required for safe and secure behaviour (Rastogi & von Solms, 2012) in safeguarding IS resources. Hence, they formulate security policies and controls based on technological consideration only (Ciampa, 2014:88). This is then the only defences for IS resources ignoring the needs of IS security e-competencies development among end users (Rastogi & von Solms, 2012).

Thus, the need arise for management support and buy-in beyond the mere approval of training. The approval of training and development budget for end users and to be a role model for security initiative has a far more positive influence in the rollout and success of security initiatives (Hayden, 2010:274,341-345). This is part of good governance advocated by the King Report III as it include the security of IS resources in its list of responsibilities of executives (Ungureanu, 2013) and form part of corporate governance (Johl et *al*., 2013).

6.4 CHAPTER SUMMARY

From the data analysis it is evident that currently in HEIs, security of IS resources is more about the technologies than people (end users). This is obtained from the perspective of the four participating HEIs. Likewise, this conclusion is confirmed by the fact that currently, the HEIs do not provide formal IS security training to end users to develop their IS security e-competencies. As a result, there is a higher probability that they would have a deficiency in handling critical information and those related to intellectual properties of the institutions or their business partners.

In addition, the participating HEIs face various challenges that need to be addressed to ensure that the development of IS security e-competencies is a successful undertaking. One of those challenges is to address the failure of the university council (which is the company's board in the HEI) to address the issue from its strategic point of view in the security policy or to come to the decision that as HEIs are not financial institutions, IS security does not matter. However, with the introduction of new laws such as POPI, the nature of the organisation does not matter, as long as the information is collected form the stakeholders, the protection

of this information has become a mandatory exercise, and the development of IS security e-competencies among the end users becomes an unavoidable exercise.

In the next chapter, the framework for IS security e-competencies development among the end users in the HEI is proposed. Alongside, consideration is given to job requirements, levels of end users, needed competencies, and the method through which the competencies can be supplied to reach the majority of end users also taking into account the challenges the HEI environment holds.

CHAPTER SEVEN: FINDINGS AND DISCUSSION

7.1 INTRODUCTION

The previous chapter (Chapter 6) presented a thorough discussion of empirical data collected through in-depth interviews (qualitative research), which were supported by research questionnaires (quantitative research) from the four participating Higher HEIs from the Western Cape Province. In addition, the data collected from the ICT security practitioners from other seven HEIs were added to support the relevance of IS security e-competencies to be developed in the HEI context.

This chapter summarises the findings of this research in relation to the exploration of IS security e-competencies practices of the four participating HEIs (HEI01, HEI02, HEI03, and HEI04) and the development of the IS security e-competencies development framework for end users in the HE context.

7.2 EMPIRICAL JUSTIFICATION OF THE STUDY FROM THE PRACTITIONERS PERSPECTIVE

Before engaging in details on the solution to this research question, it is important to reiterate the answers collected during the interviews with the nine ICT security practitioners from the other seven HEIs. They were consulted to understand the importance IS security e-competencies for end users in the HEIs, as well as to identify the needed competencies to protect their individual information, the respective institutions' information, and the IS resources that process and transmit the information.

The themes that emerged from interviews with the ICT security practitioners are summarised below:

- When asked about the importance of IS security e-competencies for the end users of IS resources, the nine ICT security practitioners said that the security e-competencies are important for end users of IS resources and everyone who is using IS resources need to be trained on their security.

- When asked to review the importance of aspects of IS security in the organisation like security technologies, security training, security policy, security culture, physical security, and security cameras; the ICT security experts asserted that these aspects of IS security are important for the protection of IS resources.
- Another important question asked to the practitioners was to identify the IS security e-competencies that can be supplied to the end users. These IS security e-competencies were classified in the four spheres which are presented in Table 7.1 with frequencies produced from Atlas.Ti as suggested in Tshinu et *al*. (2014).

Table 7.1: Spheres of IS security e-competencies content

Spheres	**Frequencies**
Sphere 1: ICT security policies and procedures	19
Sphere 2: Environment (Internal and External)	20
Sphere 3: Security technologies	12
Sphere 4: Culture	8
TOTALS:	**59**

From the experts' information, the content for IS e-competencies development for end users is more grounded in the non-technological aspects than for the technological aspect. The full list of the training content is presented in Appendix E. As presented in Tshinu et *al*. (2014) the review of published articles and books (as part of this research publication), it was discovered that security policies and procedures sphere, and environment sphere present frequencies of 35 and 32, while security technologies and culture show frequencies of 26 and 7.

Apart from the importance of IS security e-competencies and the four spheres of IS security presented in Table 7.1, the practitioners mentioned also the important challenges that HEI face during the process:

1. There is a common practice in the HEI environment that constructs the process of IS security as a whole. This is even bigger than what it appears like given its line of operation. In fact, social networks are vulnerable to ICT

security threats and are blocked by other commercial organisations. In the HE environment, these social networks are open for educational purpose. As such, the HEIs are opened to more security threats and need a holistic and better multi-layered ICT security than commercial organisations.

2. The experts also added that HEIs teach students about viruses and how they are transmitted. As part of learning, students have to develop and execute these applications (viruses) to see their effects on the systems. In this regard, the institutions become more vulnerable than other organisations because of this core teaching and learning business.

7.3 SUMMARY OF THE FINDING

The summary of this research is presented according to the three main categories of research objectives and research questions. Each is discussed with its sub-objectives and is translated into questions discussed with participants during the interviews and questionnaires that were distributed to the end users. As presented in Chapter 1 and analysed in Chapter 7, the main summary is presented according to the three main sub-objectives and presented below.

7.3.1 Sub-objective 1: The analysis of the importance of IS resources and their security in the HEI environment

Under this category the following three sub-objectives were achieved:

1. To explore the importance of IS resources in the operations of the HEIs. The key themes were:
    - IS resources are important for the running of HEIs administration, research, and teaching and learning as none of these aspects can be run effectively without the ICT platform.
    - They help in the processing and distribution of information from registration and examination, to the graduation and those of employees.
    - They help in the protection of research data that has strategic value for the HEIs and the nation (including military research and those run in collaboration with partners such as pharmaceutical companies).

- The HEIs communicate with students and other stakeholders through ICT service like e-mails which are more effective.

2. To determine which ICT systems in the HEI environment are critical and have been classified as such and support the operations of HEIs. In addition to the importance of IS resources in general to the HEIs, the HEIs run critical ICT systems that require the end users who access them to be IS security e-competent (apart from security technologies). This competency is necessary to protect the information that are accessed as well as other IS resources. The critical systems include:
   - The general administration systems such as HR system, students' administration system for the awarding of qualifications, the financial system (ERP), and the procurement system.
   - The teaching and learning management system (ERP system) that keeps student information and records, black board or e-learning system.
   - Communication systems such as the e-mail system.
   - The general infrastructure such as the network, computer systems that support teaching and learning, academic administration, and research.

Apart from these systems, the end users who are also the custodians of the information are also critical resources to the HEIs and the security of information and other IS resources.

The understanding that the above-listed systems are critical to the operations of HEIs is purely based on the perception that respondents hold. This is not based on a formal classification of IS resources according to their criticality, except in certain cases where encryption was done at that managers' level.

Apart from the qualitative data, the quantitative data were also collected from the end users to explore how important the IS resources are to their work. From the question "I rely on my computer and other IT resources to do my work", it was observed that a combined percentage of 97.3% of respondents

agreed and strongly agreed. In addition, 79.2% of participants reported that they also use their own computer or mobile phone to access e-mails and connect to their institution's network off the campus.

The above summary shows that IS resources are important to the operations of HEIs as both qualitative and quantitative data support this view.

3. To explore from the ICT security experts and end users in the participating HEIs whose responsibility is it to protect the IS resources. From the information gathered it was summarised that:
    - From the qualitative data, the security experts from the four participating HEIs agreed that end users of IS resources form an important part of the security of IS resources accessed.
    - From the quantitative supporting evidence, a cumulative percentage of 42.8% believed that IS resources security is either the responsibility of end users or a shared responsibility between end users and ICT technicians. A cumulative percentage of 57.1% of participants believed that the IS resources security is not their responsibility, but the responsibility of IT technicians.

Besides the recognition of the importance of IS resources in the operations of HEIs for instance research, teaching and learning, and general administration, the majority of end users still do not recognise that the security of IS resources is their responsibility. This lack of insight into responsibility for the protection of IS resources is one of the aspects of IS security e-competencies development that need to be addressed in this research.

The conclusion drawn from the category 1 section is that IS resources and their security are not just important for financial or military organisations. But because they carry important information that is considered as the lifeblood for HEIs, these systems become important and core to HEIs (Sarkar, 2010; Calder, 2013:13). Given also that HEIs carry out important research that have significant value for their financial income, and are strategic to the country (like military researches), or for

pharmaceutical companies, the development of IS security e-competencies of end users through training and the raising of awareness become important (Tsohou et *al*., 2012; von Solms et *al*., 2011; and Steenkamp, 2011).

Concerning IS resources security responsibility, Piccoli (2012:32) demonstrate that end users are at the centre of the operation and protection of all the IS resources. In addition, Ungureanu (2013) also states that the security of IS resources that end users access and use is important and it is not just the responsibility of security technicians. End users and executives need to be involved at different levels. Besides, given the existence of multiple threats to IS resources, their security has become the responsibility of everyone in the organisation (Sedinić et *al*., 2014; Whitman & Mattord, 2010:2, and Humphreys, 2008). Although the majority of participants in this section hold the opinion that ICT technicians have the responsibility to secure IS resources against threats, it is evident that perception change is needed in this regard. This change can be formalised only when HEIs determine the IS security e-competencies in a formal framework that takes account of end users' needs.

7.3.2 Sub-objective 2: The exploration of IS security e-competencies development practices as practiced by the four participating HEIs

Besides discovering the importance of IS resources, their categories, and the importance of their security in the HEI environment, the category focuses on the exploration of current IS security e-competencies development practices of the four participating HEIs.

For this purpose, the following objectives were achieved:

1. To determine if the end users have been formally trained in IS security at their respective HEIs. The common themes that emerged from the interviews with participants include: a) the institution falls short on IS security training; b) no formal IS security training has been provided to the end users; c) some exposure may be done during the induction but it is not a coherent exercise; d) there is no formal IS security training done, but they incorporate some

aspects such as the importance of password during general SAP training; and e) the IS security training is critical but it has been neglected.

Except for the interviews with the IS security representatives from the four participating universities, two questions were asked to end users of IS resources too, namely if they have received any formal IS security training. From the 385 participants who received the questionnaires, none of them was formally trained by the institution on IS resources security. Only 8% of participants (or 31 participants) did receive IS security training but as part of their personal development or from the other employers.

From the investigation and the data collected through interviews with IS security experts and other representatives, it was confirmed that the participating HEIs do not provide any formal IS security training to the end users, not even to those that are using critical systems. This clearly is not in line with the best practices that authors suggest in proposing that the only way of enforcing IS security in an organisation is when proof can be given that the end users have been reached in the particular organisation (Whitman & Mattord, 2014:148) as the existence of security technologies cannot protect against human weaknesses and behaviours. In the latter case, the end users are still the greatest threat and vulnerability against the IS resources (Kouns & Minoli, 2010:3).

2. To explore the challenges that HEIs are facing that affect the development of IS security e-competencies. As the end users of IS resources are not trained on IS security, this question asked the IS security experts and the other participants to highlight any challenge they face in their particular HEIs that directly or indirectly affect the development of IS security e-competencies.

   From the interviews, the following themes were collected:

   - The struggle to come to agreement with the executives on the importance of IS security and the involvement of heads of departments.
   - Lack of resources and personnel such as the IS security officer who can take charge or coordinate the IS security operations, talk to various

groups, and organise workshops. It was found that all the four participating HEIs struggled to attract this resource (IS security officer) and some opted for contracting consulting services.

- The integration of different departments to ensure that the IS security practices are included in the contract. Also to insure that proper actions are established when there is breach of contract instead of acting in piecemeal.
- People not reading policies and other communications posted online is another challenge that HEIs experience.
- Limitation on budgets to finance the recruitment of security personnel was also mentioned.

The above challenges have a direct impact on the formal development of IS security e-competencies among the end users of IS resource. This is also true though the IS security programme is to be implemented.

With regard to the challenges, it is the university councils (representing the board of the company) through their committees who is in charge of IS security. They have to recognise the importance of IS resources and their technological security, as well as the integration of the end users of IS resources in the IS security programme through IS security e-competencies development strategies (von Solms et *al*., 2011; Ungureanu, 2013).

The inclusion of IS security training for end users in their security policy (which does not exist currently) and ensuring that the council and management set a good example in supporting the IS security training programme. If management does not support it in such a way, it could be widely undermined (Whitman & Mattord, 2010:200).

3. To determine the major threats affecting the IS resources in the HEI and how they are dealt with. The following themes on threats were identified:
    - Concerning the sources, the threats facing IS resources in HEIs are from both internal and external sources.

- The threats from internal sources are the most dangerous and difficult to control. This is because internal users have knowledge of the systems and have access (authorised) to lot more than people external to the HEIs.
- Among the threats that IS resources face in the HEIs include viruses and malware attacks, social media accounts exposing the institution, social engineering, people not taking responsibility for the IS resources (including information), fear for compromise of exam papers as they are on the network, altering students marks, uploading confidential information in public folder, and IS security e-incompetent end users who cannot identify the security threats.
- Lack of resources such as IS security officer to attend to threats, monitoring across systems and lack of proper enactment of IS security policy were considered as threats in HEI.
- The threats in general cost the HEIs down time, loss in productivity, embarrassment and damage to the reputation especially when degrees are given to undeserving students or acceptance letters are sent to non-accepted students.

The end users from the four participating HEIs were asked if they are able to identify the security threats that affect the IS resources they access in their environment. Out of 383 participants who completed the questionnaires, 308 participants or 80.4% said that they will not be able to identify the threats affecting the IS resources in their environment. There was also no difference in reference to these answers of end users on this question among the HEIs that answered this question with significance $p = 0.271 > 0.05$.

The ICT security experts and their representatives also mentioned that the external threats are easily controlled through security technologies. However, the internal control cannot be contained through security technologies, but mainly through security training, policies and procedures. The latter require also training and some sort of awareness as it is difficult

to ensure that end users do read and understand the content of ICT security policies.

To enforce the fight against the ICT security threats in the HEI, authors recommend proper supervision, security training and awareness on security issues (Ettinger, 1993) The emphasis on ICT security policy which articulates the end users' behaviours, goes beyond the uploading of ICT security policy on the network system (as it is the current practice in HEI). Also It is also to ensure that employees read, understand the content, sign the policy and related sanctions, and provide training to end users (Piccoli, 2012:395; Humphreys, 2007).

The current practices as discovered during the interviews reveal that the participating HEIs fight security threats mainly by using ICT security technologies such as firewalls, IPS, and antivirus applications. They also rely more on access control and the separation of access to critical access. The formal ICT security training of end users to develop their IS security e-competencies is either totally forgotten or non-existing.

4. To determine how the ICT security experts rate institutions' commitment to the development of IS security e-competencies. As the participating HEIs do not have official IS security training programmes or have a formal session to discuss IS security related security issues, it was not surprising that the rating was in general not satisfactory.

   In general, the following themes were collected from the ICT security experts or their representatives from the four participating HEIs:

   - The IS security e-competencies development is at its start-up.
   - We are very far from what we want to do concerning IS security e-competencies development.
   - We understand security but understanding the security landscape is difficult and that is where we lack. We can run more IS security awareness campaigns.

- There is intent to develop end users IS security competencies, but there is not sufficient commitment.

All the ICT security representatives of the four participating HEIs low-rated their respective HEIs commitment to the development of IS security e-competencies. This confirms that institutions are doing even less for IS security e-competencies development.

With regard to the development of IS security e-competencies in HEI, there is a need for enforcement from the organisation leaders and senior executives through ICT security policy (Henry, 2004 as cited in Thomson & von Solms, 2006). Chapman et *al*. (2010) confirm that management involvement and accountability has an influence on employees' behaviour in IS security. Therefore, the participating HEIs' councils and senior executives (through their ICT security committees) have a responsibility for setting a strategic direction, allocate resources, and support the programme to stimulate the end users' commitment and behaviour change. This should also set the pace for developing their IS security e-competencies.

7.3.3 Sub-objective 3: Summary of data from the exploration of optimal ways of supplying the needed IS security e-competencies in the HE environment

The objectives related to the supply of IS security e-competencies to end users were achieved and discussed through:

1. The exploration explore who are the key end users of IS resources and how can they be classified in terms of their responsibilities and the need for IS security e-competencies: From the information collected on this objective, the following themes were identified:
    - Everyone who is using the IS resources in the HEI environment (from students to staff members, NGOs, and contractors) who access IS resources are key end users.
    - The systems administrators are critical end users due to their access to almost everything.

Concerning the categorisation of end users (mainly staff members in the end user department) for the purpose of IS security e-competencies development in the HEI, this research identified the following three levels of end users:

- Level 1 comprises general end users such as general administrative staff members and academic staff whom access information to perform their duties.
- Level 2 consists of information managers (information officers) who are called super users for information in certain departments. They are tasked with the implementation of policies with a particular end user department. To this level, this research adds the departmental officers such as the financial officer and procurement officer who, because of their positions, have to authorise transactions of large amounts.
- Level 3 are the departmental heads (called information curators) who set the roles, access right, and operating procedures for information in their departments. The information curator can be the financial director if it is finance information, HR director when it is human resources information, and the registrar in regard to students' information.

Concerning the administration of information in the HEIs, the IT department has the responsibility limited to the provision of infrastructures and the security of the infrastructures. The individual department is responsible for the control of its information. Hence, the IT department and other authorities in the HEI, such as vice chancellor, have a limited access to information.

In line with the IS security e-competencies development framework, the identification of the competencies levels (categories) of key end users is a key step as it was identified as a step 5 for the creation of a competency framework (Holt & Perry, 2011:103-121). The identification of security e-competencies levels is also an important step for the provision of appropriate competencies required by individual end users (Morelock, 2012; Sedinić et *al*. 2014). In other words, Turban & Volonino (2012:131) emphasise the importance for grouping the employees for IS security training according to

their jobs and how these aspects relate to their work environment and operations in the HEI environment.

2. To explore the importance of IS security e-competencies development for the end users and the institution: The key theme collected from this sub-objective was that the development of IS security e-competencies for end users is an important part of the IS security measure for the HEI. Unfortunately, this is not being done currently. Most important is also the insurance that end users understand the laws related to the information protection such as PAI, POPI, and ECT acts, and the disciplinary process related to the mishandling of IS resources.

   The end users were also asked if IT security competencies were relevant to their work. Out of 385 participants who received the questionnaires, 379 participants answered the question. From the total, the sum of 266 participants (or 70.2%) affirmed that IS security e-competencies are important for them and the IT resources they access. This high rate of agreement is one of the reasons for end users to attend the IS security training. This should also encourage HEIs to provide end users with the needed IS security e-competencies.

3. To determine the challenges experienced when training staff members in the institution: These challenges are specific to the training and development of the four participating HEIs. Also, this could negatively affect the development of IS security e-competencies.

   On this sub-objective the challenges were grouped in the following themes:
   - The limited budget and number of people allocated to the training and development.
   - All four participating HEIs have various campuses, service sites, and employees are dispersed across the Western Cape Province. To allocate employees in one location for training is challenging. This can

be solved through a strategy that adopts additional methods of the training to be combined with the contact mode.

- Getting the right people in classroom for training was another challenge that participants mentioned, as there is no system that can help in the continuous matching of skills and training programmes.

In relation to the challenges in the training and development, the addition of IS security e-competencies development programme would need extra funding and coordination, hence a supplementary budget. This corroborates with the suggestion that globally, security training and awareness programmes either do not work sufficiently or the investments made in the programmes are inadequate (Tsohou et *al*., 2012).

4. To determine the content of IS security e-competencies development from the ICT security experts' point of view: On the content of IS security e-competencies development the following themes were collected from the ICT security representatives:
    - Basic understanding of security technologies and threats: training on the viruses and how to deal with them, scanning of external storage devices and their computer, and also information on the firewall.
    - Awareness about environmental security (internal and external environment): proper management of user environment as it is done with a financial ATM card, inform end users about the threats to IS resources both internally and externally, knowledge of external environment and acts such as PAI, POPI, ECT, and the HE Act that affect the way they deal with information and related IS resources.
    - Awareness about procedures and policies: proper selection and protection of the login details such as password control, and logging off after the session, knowledge of who to contact in case of security threat (possibly give the telephone number), be trained on the content of security policy and related policies, access right to information.

Even if the knowledge of the implications for mishandling information and other IS resources is not part of IS security e-competencies, end users also need to be made aware of the consequences of not applying the IS security rules and procedures. It is of utmost importance that end users take ownership of their information and actions such as if they do not log off after accessing the critical systems.

On the subject of the IS security e-competencies content, end users were also asked if they understand the legal implication of their actions on IT resources. Out of 385 participants who received the questionnaires, 383 participants answered the question; among them, 310 participants (or about 81%) disagreed, did not know, or strongly disagreed that they do not know the implications of their actions on IT resources security. As in the case of knowledge of legal requirements, end users have to know that the use of information for unintended purpose for which it was collected for is illegal and can result in disciplinary procedures. This knowledge can help them to refrain from illegal activities and contribute to proper usage of information and other IS resources.

From this understanding it can be concluded that the implementation of IT security technologies alone cannot solve the security challenges and threats that HEIs face. It is necessary to also provide the non-technological security e-competencies in the protection of IS resources (Alfawaz et *al*., 2010).

5. To explore the current practices and approaches to training that the training and development department and the institution adopted in providing training to employees: The current practices have an impact on the development of the IS security e-competencies. The identification of these practices can help to either avoiding the practices or strengthening them to support the IS security e-competencies development for HEIs with employees dispersed across various campuses and service centres.

With the knowledge that four participating HEIs do not provide formal IS security training to the end users of IS resources, the following themes were identified on the current training and development practices:

- The access to the ICT security policy is through the online or LAN, and one challenge that these institutions are facing is that end users do not read policies and other communications sent either through e-mails or uploaded on the local network. Hence, it is difficult to rely on the information provided through newsletters, e-mails, and those uploaded online that they help in creating effective awareness on IS security.
- The ICT security representatives do provide update information on viruses to end users through newsletters. This focuses on basic advice such as do not open unrequested e-mails with .exe files. Again, end users read the electronic communications with difficulties or do not read them at all. To another extent they cannot identify an .exe file.
- The four HEIs have an induction programme through which new employees are introduced to the institutions' processes. This induction can be used as a platform for providing formal IS security training.

From the current practices, the four participating HEIs rely more on newsletters and e-mails to remind end users and update them on the viruses and other ICT related threats. Even though this option is one of the recommendations for creating awareness on ICT threats, it is only effective after end users have been trained as it reminds them on already established knowledge or on knowledge that would not be difficult to recall. In this regard, Eminağaoğlu et *al*. (2009) mention that an awareness campaign (such as distribution of newsletters and e-mails) should be added to training courses to complement the training. This should be done as employees tend to forget the content they were exposed to during the training.

6. To explore the methods used to provide training to employees in the HEI environment and their effectiveness, there are methods to meet the current needs and those of IS security e-competencies development: Currently, the

four participating HEIs mostly use the contact mode (classroom method) for the training of their end users.

While the classroom method offers advantages such as the possibility for participants to ask questions and the opportunity for learners to learn from one another, its disadvantage include the limitation to attract participants who are situated in other campuses and sites and cannot attend training. The question on training method preference was also asked to the end users to select the preferred method or mixture of method. The preferred method was contact mode (57% of participants), followed by online training method chosen as preferred method (with 36% participants).

To ensure that IS security e-competencies are developed to include end users that are dispersed across different campuses and sites, the literature recommends the mixture methods to accommodate different learning styles (Lucas, 2012). Furthermore, in such a case the end users who are dispersed across various campuses and sites can be accommodated. In addition to contact and online methods, the inclusion of mandatory IS security e-competencies development training during the induction workshop was proposed, An IS scenario plus questions at the beginning of each semester as part of the programme was also suggested. These methods can be supported by the newsletters, e-mails, and other communications that are distributed to the end users during the year to raise their awareness and develop their IS security e-competencies.

Finally, from previous research support is given to the importance of IS e-competencies development for end users. Piccoli (2012:32) mentions that end users are at the centre of the operation and protection of all the other IS resources (including information) as they are currently in the HEIs. Lynn (2009) assures that security technologies (hardware and software) means nothing if end users do not practice cyber safety (or take care of IS resources) as some threats are human-related for instance errors and negligence (Wood, 1995). Other human-related threats include carelessness in handling access details and critical IS resources, and

information (Rainer & Cegielski, 2013:85-86). These cannot be prevented by security technologies but through IS security training, awareness, and security policies and procedures in which end users need to be trained.

7.4 IS E-COMPETENCIES DEVELOPMENT OVERARCHING ACTIVITY SYSTEM (OAS)

From the perspective of data that were gathered, it has been discovered that IS security e-competencies development takes place in a social environment which is why the OAS Activity Theory (AT) is constructed from various concepts that interplay to achieve a common object of developing IS security e-competencies of end users. This is presented in Figure 7.1 that highlights the areas that HEIs need to improve to effectively develop the IS security e-competencies of IS resources end users.

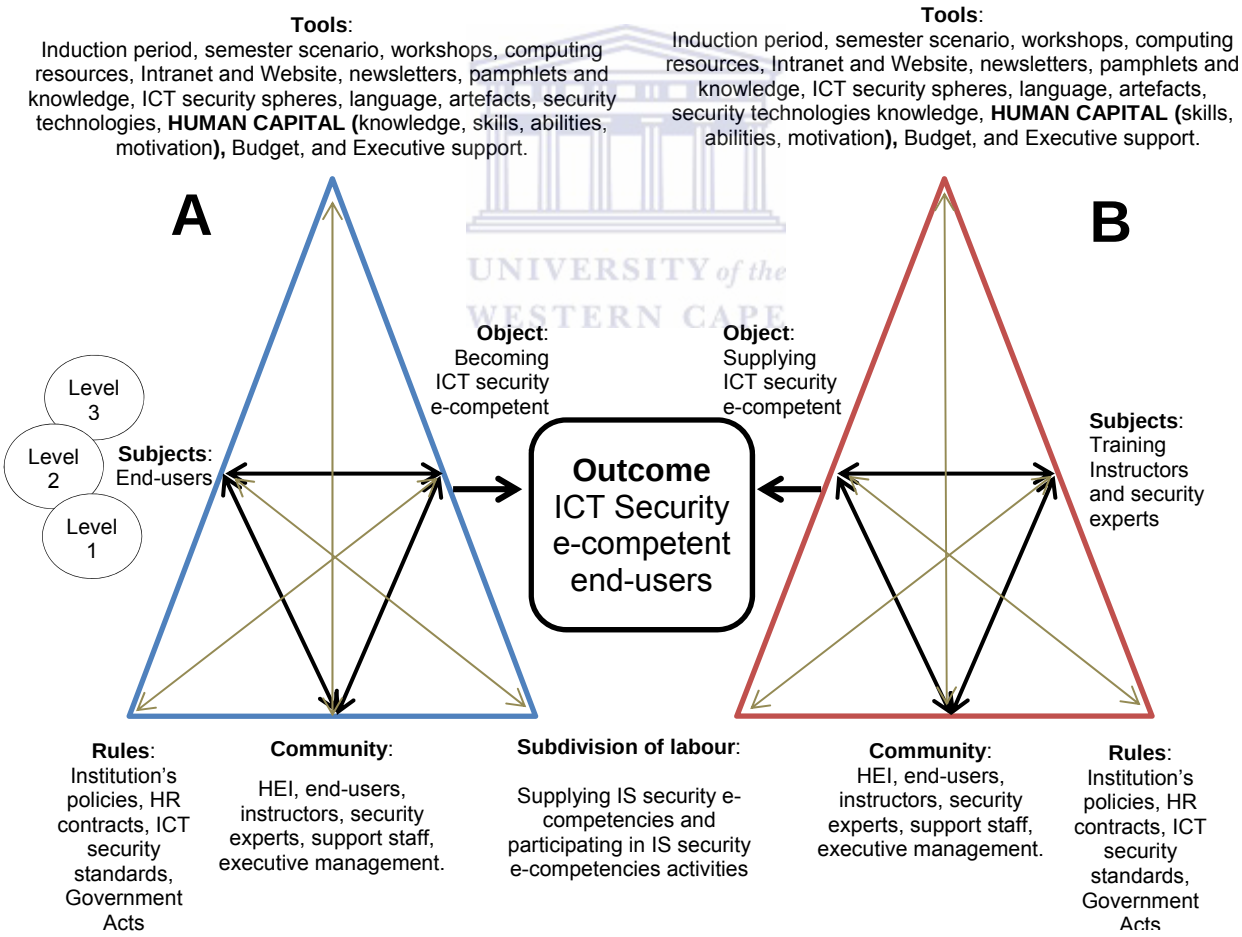


Figure 7.1: IS security e-competency development OAS

Source: Adapted from Clark & Fournillier (2012), Allen et *al*. (2011), Paraskeva et *al*. (2010).

Figure 7.1 can be explained in the context of IS security e-competencies development in the HEI context according to the explanation of AT components as provided in Chapter 5:

- **Subjects**: In the overarching Activity System (OAS), the subjects are both the end users who need to develop their IS security e-competencies and the trainers who provide training. From end users' point of view, there is a need in terms of competencies framework development to subdivide them in levels which are necessary for the targeted IS security e-competencies supply. Currently, the four participating HEIs neither identified nor classified the subjects.
- **Tools:** There are many tools that intermediate between the subjects and the object they are achieving. Among these are the digital tools and related process, which according to Ala-Mutka (2011) intermediate in all types of tasks and are parts of competencies in the IS security e-competencies development. There is also a requirement for budget, and the support of IS security e-competencies development from the university council and executive management.

  As the practices are current, the four participating HEIs cannot successfully achieve a positive outcome in the development of IS security e-competencies as they are under-resourced (in HR and financial). Thus, they need to officially integrate the IS security e-competencies training in the induction programme. They need to combine the contact and online methods to ensure that the programme reaches employees who are situated at other campuses and sites.

- **Rules**: Among the rules and documents supporting the development of IS security e-competencies, are the HEIs' own security policy and other related policies, government Acts such as PAI, POPI, ECT, the HE act, and any other best practice such as the King Report III. Also included are standards such as ISO27002 that can be used to regulate the achievement of the object of e-competencies development. Currently, end users (subjects) have no full

access to these rules or have never officially been provided an official training on standards to know and apply the content.

- **Community**: This component reflects where the end users and the training providers come from. It is mainly the HEI and the community from which the end users come from. The community of end users and subjects exist, but this community is general and has not been classified or properly identified for the supply of IS security e-competencies.

- **Division of labour**: This is very important for training as the members participating in the training need to know their roles and responsibilities. In this research there are two main groups in the division of labour, one receives the IS security e-competencies (the end users) and the other supplies the IS security e-competencies (ICT security representatives).

  In the current setting, the four HEIs surveyed find it difficult to divide the labour on IS security e-competencies development. This is because they lack resources such as finances to attract an IS security officer who can coordinate the IS security e-competencies development activities.

- **Object**: In the case of this research, the object of the activity is for the end users to become IS security e-competent, and for the suppliers object, it is to ensure that they supply the needed IS security e-competencies. Given the lack of resources (challenges) and shortcomings on other constructs identified after the application of the Activity Theory (AT), it is difficult to believe that the surveyed HEIs are able to achieve the object of IS security e-competencies development.

- **Outcome**: The expected outcome of an activity is to ensure that end users are IS security e-competent. However, to reach this object there is a need to ensure that all the constructs are available in quality, good quantity, and ready to be used. Otherwise, the outcome cannot be achieved.

Interpreting the IS security e-competencies development in the HEI, using the Activity Technology (AT) as theory, demonstrated that it is a complex and multi-level undertaking that can be understood through the system approach. The model recognises also the complexity among the constructs of IS security e-competencies (subjects, tools, rules, community, and division of labour) in their drive for the achievement of the activity systems object.

As demonstrated in the Figure 7.1, end users have to successfully achieve the object of their activity system. The object in the supply side of the activity system need to be successfully achieved, otherwise the IS security e-competencies cannot be successfully developed.

Adopting the AT for executing this research is founded in the following facts:

- The IS discipline approaches knowledge from a soft issues perspective rather than from hard issues as it deals more with interaction between people, organisations, and technologies and not technologies themselves (Avison & Pries-Heje, 2005:189).
- The AT understands that the development of IS security e-competency is only possible if there is commitment from different stakeholders taking part in the activity with supporting resources and tools. Otherwise, the achievement of object of the activity would be impossible.

In relation to this research paradigm stance and the paradigm model of Rastogi & von Solms (2012), the ICT security manager and staff in the institution are considered as both experts (functionalist paradigm) and catalyst or facilitators of IS security e-competencies development among the end users (Interpretive approach). With regard to end users, instead of being inconsiderate towards the impact of end users, their working practices, and needs for security requirements (functionalist approach), the emphasis needs to be on end users' willingness to learn, accept ICT security policies and controls (interpretive paradigm) (Rastogi & von Solms, 2012) and participate successfully into the IS security training programmes.

The above considerations on research outcome would enable the participation of end users in the IS security programme to create a truly holistic approach to IS security in the HEI environment. This contrasts the functionalist approach which is more mechanistic, technologically focused, and lack the participation of end users.

In general, the approach to IS resources security in the HE environment should follow the principle of Jirasek (2012) who quoted Boyd "It is all about people, process, and technology". However, people are the biggest and the most vulnerable among the three components (Okenyi & Owens, 2007) as people make, use and maintain the IS resources (Hayden, 2010:272-273). In their interactions with the IS resources and related security, if people do not possess appropriate knowledge and there is no cooperation from the end users (people), these security tools can be misused or misinterpreted (van Niekerk & von Solms, 2010). As a result, they become useless for the intended purpose of protecting IS resources from misuse and threats.

The following section (section 7.4) presents the IS security e-competencies framework that HEIs can refer to when implementing the IS security e-competencies development programme for the end users of IS resources.

7.5 THE IS SECURITY E-COMPETENCIES DEVELOPMENT FRAMEWORK

After the analysis of data collected from the literature review (Chapters 1 to 4), and the analysis of the artefacts contributing to the successful development of IS security e-competencies through the Activity Theory (AT) in Chapter 5, and the review of empirical evidence from both experts and end users (Chapter 7) through the application of a mixed research method (Chapter 6), certain gaps related to how IS security e-competencies were identified by the end users in the four participating HEIs and indicated as needed to be addressed.

From the gaps identified, the foremost is the failure from the participating HEIs' university councils to provide strategic direction on the IS security e-competencies development. Further is the lack of formal training of end users on IS security, non-categorisation of critical information and resources and end users, and advising the

end users on the importance of such categorisation. These gaps resulted in the undertaking of this research and the development of IS security e-competencies development framework (Figure 7.2). Also developed, is supporting frameworks that present components that need to be rectified in order to address the IS security e-competencies in the HEI environment.

The implementation of the proposed IS security e-competencies development framework provides a detailed outline and serves as a starting point for HEIs to design, select practices, and implement the IS security training and education, and also the awareness campaign (Whitman & Mattord, 2014:212-219). The implementation of such a framework is a demonstration that HEIs are keen to secure business practices (Siponen & Willison, 2009), which addresses both technological and non-technological (human or end users) solutions.

SEP06 from HEI04 mentioned that the report from the recent audit of their IS practices recommended the adoption of related ICT management frameworks such as COBIT and IT Governance. According to the respondent, *"the adoption of such framework can provided best practice we can learn and implement"*. This research believes that the development of IS security e-competencies framework, specific to HEIs, will be even more advantageous as it recognises the challenges and needs of these HEIs for IS resources security.

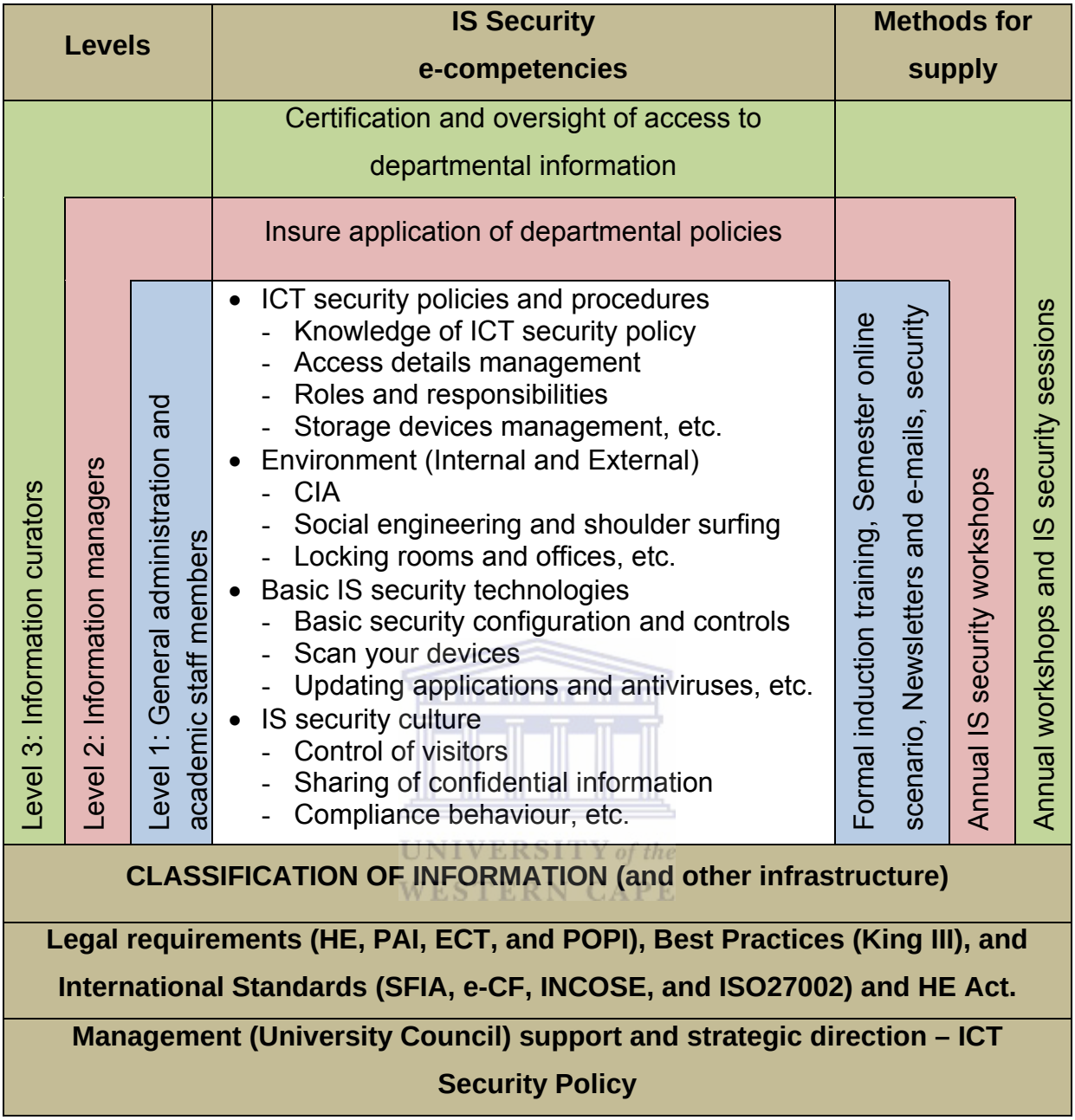


Figure 7.2: IS Security e-competencies development framework for end users

The presented Figure 7.2 represents the IS security e-competencies framework that can help to address IS security e-competencies for end users of IS resources as opposed to other frameworks such as Skills Framework for Information Age (SFIA) that address the skills requirement for IT professionals. The framework presented in Figure 7.2 is intended to address the following elements that make up its components:

- Management support and strategic direction;

- The best practices frameworks and legal requirements;
- Classification of IS resources;
- End users levels;
- IS security e-competencies; and
- Methods of supplying the IS security e-competencies.

The Activity Theory (AT) which was used as a conceptual framework which was further expended to Figure 7.1 helped in the development of the framework (Figure 7.2). In particular, the analysis of components such as levels of e-components which the subjects need to develop, the IS security e-competencies, and the tools that are used to facilitate the e-competencies development, and the rules that need to be respected such as institution's policies, standards, and Acts that apply in the process of IS security e-competencies development.

The framework presented in Figure 7.2 was put together by considering input from different sources:

- From the Activity Theory (AT) which was used the lenses through which the IS security e-competencies development in HEIs was analysed and its foundation conceptual framework helped in the discovery of the components of the Overarching Activity System (OAS) and how they contribute to the development of IS security e-competencies.
- The literature reviewed informed the creation of the framework (Figure 7.2) as the understanding of IS security e-competencies and the supporting rules such as frameworks and policies was derived from the reviewed literature.
- The interviews and the surveys that were conducted with the participants helped also in the discovery of the gap between the current practices and the proposed framework, the determination of IS security e-competencies requirements, and the importance of such framework in the HEI environment.

The components of Figure 7.2 and their contribution to the development of IS security e-competencies among IS resources end users are discussed in the following section.

7.5.1 Management support and strategic direction

A successful implementation of IS security e-competencies development depends on the support that the programme receives from the management and their setting of strategic direction from the ICT security policy. The security policy is approved by the board (University council) and it is a high level document that is used to communicate the organisation's business and security objectives (Jirasek, 2012). It is also a document through which the security threats' countermeasures and penalties for breaching the security measures are communicated to IS resources end users (Yildirim et *al*., 2011, Whitman & Mattord, 2010:118-121).

The King Report III (of 2009) places the responsibility for IT governance on the board of the organisation. In its recent publication, the King Report III included the aspects of IS resources security in the list of responsibilities for the management (Ungureanu, 2013). In this research, the university council through its ICT committee has the responsibility to provide a strategic guideline and support through ICT security policy on the IS security e-competencies development.

For the ICT security policy to be effectively implemented, it is required to be distributed to the end users as well as be regularly assessed or evaluated to ensure that end users are aware of its existence and apply its content (Ahlan & Lubis, 2011). Employees must acknowledge it by means of a signed consent form, which is better done after employees have been trained on it (Whitman & Mattord, 2010:194-195) as they need to understand its content. Therefore, everyone in the HEI should be convinced, taught, and continuously made aware of the rules and regulations established in the ICT security policy (Whitman & Mattord, 2010:136-143; Humphreys, 2008) and why it is relevant to the organisation.

Currently, the ICT security department has a challenge in getting the management to support the importance of certain ICT initiatives. Employees are not trained due to the lack of resources and strategic guidance, and the employees are referred to ICT security policy that is uploaded online and which does not cater for the training on IS resources security. One of the challenges experienced in IS security management is

that employees do not read the policies or read selectively. Thus, it is necessary to train end users on ICT security policy to prevent the ignorance claims.

7.5.2 The best practice frameworks and legal requirements

The reference to the best practice frameworks (such as ISO 27002) provides an opportunity for both the management and end users to be clear and know what is expected from each stakeholder participating in the programme. Especially with the promulgation of the POPI Act, any organisation that collects, processes, and transmit business information, ICT should be aware of standards and legal requirements on IS resources security.

In this research, it was established from the four participating HEIs that none of them has fully implement the ICT security framework to direct their operations. They have either contemplated to implement the generic frameworks or just could not implement them because of the cost involved.

The ICT security frameworks need to be adapted or modified to meet the unique and specific security needs of the HEI environment and to serve as a starting point for adoption which can be implemented in policies, hardware and software or combination of both (Whitman & Mattord, 2014:212, 219) This could even be for IS security e-competencies development which is also part of IS security.

The link between the ICT security frameworks and other legal requirements and the other components of the IS security e-competencies framework development is that their selection depends on management's knowledge of them. They also serve to identify the training content and the levels of IS resources security for end users.

7.5.3 Classification of information (and other infrastructure)

The summary of the views collected from ICT security representatives of the four participating HEIs was that *in the context of their IS resources security, and the development of end users' IS security e-competencies, it was established that you need to have some sort of information classification to perform actions such as access control, encryption of data, and the compliance with the legal requirements*

such as PAI and POPI. This classification also needs to be extended to the critical IS resources that process the information. End users need to be made aware of such classification as to what is sensitive and what not.

From the interviews with the ICT security experts, it could also be summarised that such classification of information has not been done at the institutions' wide level. In few instances, this was only done at IT system administration level. The reason for this non-classification is attributed to the lack of management knowledge of importance of information classification and the IT department's objection that it is not their responsibility.

The IS security and legal representatives of the participating HEIs have responded in following way regarding classification:

- SEP01 from HEI01 said: *For the classification to be undertaken you first need to understand from business (management) what is sensitive and what is not sensitive, and we haven't driven it and I do not think it is an ICT job to do it.* The security expert continued that: "*we will implement the controls to make sure that data is encrypted but the business must tell us, and I do not think that they got that in the mind*".
- The SEP03 from HEI02 said: "*We have done some sort of classification based on data managers themselves, but it does not mean that we have done much detail than that. It should have been done, but a lot as to do with what is called data retention which is not actually our responsibility. Data retention is more to do with how records are kept and management and it is very close with what we talk about, who has access to records, who can delete a record, so that is one element of it and you categorise based on that".*
- The LEG1 from HEI01 concluded that: "*the good thing here is to understand who is responsible for processing the information and what the information is. If you look at the act it has got definition of what constitutes the information that can make one to be identified is your name, your ID, and your photo and you have to store them somewhere and use them for the purpose that you have collected them for*".

- The LEG2 from HEI02 also said that: "*there will also be a need for information classification and who has access to that information and also the use of RACI has who need to be informed? Who need to be consulted? And who is accountable"?*

With reference to the IS security e-competencies framework, the classification of information provides the foundation for building IS security e-competencies among the end users. Thus, end users need to know their responsibilities and what constitutes sensitive information in the HEIs.

Currently this classification has not been done, the HEIs deal with proprietary information and externally funded projects such as those related to pharmaceutical companies' research, military projects, medical information of patients and the employees' information which are handled daily by end users, who are themselves not trained on IS security issues. Therefore, the classification of information holds value for raising awareness and for educating end users.

7.5.4 End user levels of IS security e-competencies

The classification of end users into levels for the purpose of IS security e-competencies development is one of the key requirements (step 5) for developing a competencies framework (Holt & Perry, 2011:103-121).

The importance of the classification of end users according to their levels is to ensure that IS security e-competencies are supplied to the relevant end users and they are applied to support their job level. In the HEI context, it would be irrelevant to speak about how the authorisation of access to information is done to general lower level end users who do not authorise access to information.

The determination of end users level is also an important part of training. Okenyi & Owens (2007) and Whitman & Mattord (2010:197) also identify the importance of distinguishing the audience for a certain training level to avoid the provision of inappropriate training due to the mixture of group. In other words, even if everyone

needs training on security policy, the way it is delivered to decision makers can differ from the way it is delivered to the general end users.

In this regard, one of the ICT security experts (SEP05 from HEI04) mentioned that "*the big problem is you need to target training according to the audience*".

7.5.5 IS security e-competencies

The need for IS security e-competencies is not only a domain of ICT security experts, the pervasiveness nature of IS resources in the modern HEIs, the need to protect critical resources and business interests from research funding partners such as pharmaceutical institutions, military projects, health and employees. Information require also that the end users who come across such information be provided with proper IS security e-competencies needed to ensure the security of the information.

In addition, from both the literature (Crossler et *al*., 2013; Richardson, 2011), and the interviews with the ICT security representatives of the four participating HEIs, it is demonstrated that insiders or trusted employees present the biggest and permanent threat to IS resources. This is more so than from external people, be it by human mistake or deliberate acts. This is because of insiders' knowledge of the system and its processes, and also their ability to delete any trace that could link them to those actions.

Finally, according to Holt & Perry (2011:103-121), the high level identification of relevant competencies that need to be provided to the participants (IS resources end users) for whom the IS security e-competencies framework is developed for, is the important part of a competency framework (step 4). These competencies are linked to the level of end users and have their foundation in the ICT security frameworks and ICT security policy of the institution. A full list of IS security e-competencies is presented in Table 7.9 (Chapter 7).

7.5.6 Methods of supplying the IS security e-competencies

Besides the existence of various training methods that can be used to train employees in organisations (Beisse, 2013:495-503; Ruzek, et *al*., 2012), the four

surveyed HEIs and the IS security e-competencies development present certain challenges. These challenges include lack of resources and dispersed campuses and service sites that can be addressed only in the context of HEI.

In addition to the existence of these challenges, the literature (Broderick, 2006; Robinson, 2006; and Robertson et *al*., 2013), the ICT security experts, and the end users from the participating HEIs agreed to the mixture of various training methods to accommodate the learning preferences of end users. This is also to ensure that end users who could not attend the classroom (contact mode) training can still develop their IS security e-competencies by using additional integrated training methods.

On the training provision method, Figure 7.2 indicates that:

- There is a mixture of various training methods that are appropriate to the building of end IS security e-competencies, starting with contact mode first to give employees the chance to practice the theory, ask questions to the moderator, and learn from other students.
- For the contact mode it is important to add the online training method which is useful for the dispersed campuses.
- At the beginning and during the year use the online IS security scenario and questions to be answered by end users by a certain date (15 days), or else the access to the network is to be disconnected.
- Only then, as supportive way, uses the e-mails, newsletters, and other internal publications such as company's website and official calendar to remind end users on important aspects of IS security throughout the year.

The above-mentioned were appreciated by both learning and development departments of the four participating HEIs and the users through interviews and questionnaires. The application of the mixture of methods can support and strengthen individual methods to train the end users. These methods need to be linked to the levels of end users and the message of the training.

The proposed IS security e-competencies development framework also complies with the requirements for developing a competency framework as Draganidis & Mentzas (2006) and Holt & Perry (2011:103-121) propose. This entails to group the processes in two phases, the first phase deals with the identification of the components of the framework as discussed below:

- **Step 1 – The identification of the reason or purpose of the competency framework**: In this research it is to develop the IS security e-competencies of the end users of IS resources in the HEI.
- **Step 2 – The generation of relevant stakeholders' profile**: In the case of this research, the stakeholders included the end users, the university council, and security representatives, the legal services department, and the training and development department. They participate into the process to provide direction, financial support, coordination of activities, and ensure that the holistic approach is followed and not a piecemeal job.
- **Step 3 – The identification of the sources frame**: In this research, the source frameworks include SFIA, INCOSE, and the analysis of activities through the Activity Theory (AT) that ensured that relevant stakeholders and artefacts are identified and contribute to the object of the activity.
- **Step 4 – The identification of relevant competencies**: Referring to IS security e-competencies development, the competencies are classified into four main spheres, which include basic technological competencies, the ICT security policies and procedures, the environmental factors (internal and external), and the cultural factors.
- **Step 5 – The setting of competencies levels**: For each competency, there is a separation of what end users need to know on that particular level. In the research the three levels for which the competencies need to apply are:
    - Level 1: General end users such as general administrative staff members and academic staff members.
    - Level 2: The information managers and departmental officers who implement the policy through a particular end user department.
    - Level 3: The functional managers who are called information curators. They set the roles, access right, and operating procedures for information in their functional area.

The second phase deals with the development of the actual framework as presented in Figure 7.2 in this chapter.

The proposed framework (Figure 7.2) is important in addressing the end users IS security e-competencies. This is the first framework of this nature that focuses on the end users of IS resources in the HEI environment as opposed to generic frameworks such as SFIA which focuses only on IT professionals. It does not only identify the needed competencies, but it also addresses the way in which they can be supplied to end users given the challenges and context of the HEIs.

7.6 IMPORTANCE OF THE SOLUTION

In most cases, the reference to IS resources is made to its sophisticated capability of processing information. However, the influence and involvement of individual end users in protecting IS resources should not be ignored (Avison and Pries-Heje, 2005:185). With this reference, this research recognises that the IS security e-competency framework has its place in the design and development of IS security e-competencies to help end users protect the IS resources they access. It can also serve as a guideline in the assessment of security e-competencies levels and the following:

- The development of security e-competencies creates a sense of responsibility and awareness against the IS security threats when end users access the IS resources and increases their readiness in responding to different security threats across their levels of responsibility in the HEI environment.
- The call for end users comply to IS resources security is but one part of the solution. Users need to be security e-competent when using IS resources. For this to happen there is a need for interaction and interdependence between the various components and stakeholders in the HEI environment. This include good and enacted ICT policy, effective training and development strategy and programme, continuous awareness campaign to support the training due to a dynamic nature of IS security threats.
- The proposed IS security e-competencies development framework as it is with other competency frameworks such as SFIA (Holt & Perry, 2011:19-23) would

help the HEIs to have a common vision. It also speaks the same language when it comes to the description and supply of security e-competencies among the end users of IS resources at different levels.

- The proposed framework can also be used as a tool for skills assessment and development to determine the gap and need for training in IS security e-competencies in certain critical positions in the HEI environment. Or, for the purpose of rendering implicit knowledge explicitly (Succar et *al*., 2013) in order for the organisation to assess its capability and create common knowledge.
- The skills identified in the proposed framework are more end user oriented, which are mostly forgotten by competency frameworks as they focus more on technical skills (Holt & Perry, 2011:19-23). In fact, the framework can be used by the Chief Information Security Officer (CISO) as a starting point for discussion with HR officers to identify prospective employees who need the security required for critical positions in HEIs (Whitman & Mattord, 2010:411).
- The developed framework is important for the four HEIs that participated in this research, those in other provinces, and across the globe in general as it takes account of the challenges, competencies levels, and the context of HEIs which are the criteria for developing a competency framework that relate to a specific environment and business scenario (Saldaña-Ramos et *al*., 2014).

7.7 JUSTIFICATION OF RESEARCH FINDINGS

Security controls represent the actions, methods, guidelines, practices, procedures, policies, technical, legal, and tools (Fischer et *al*., 2012, Shaleh & Alfantookh, 2011) that can be implemented to reduce the degree of threats to IS resources. As there are many threats to IS resources that can affect their integrity, there are also a number of security measures that can be implemented to protect the IS resources.

Whitman & Mattord (2010:335) perceive that the ICT security controls are classified into two spheres. One is the technological focus, which deals with security protection systems, and monitoring systems. The other is non-technological related controls with focus on end users and managerial processes such as security planning activities (related to incidents response, disaster recovery, and business continuity),

education and training, and also policy and law. These security measures can take the form of preventive and reactive technologies and non-technological controls (Rainer & Cegielski, 2013:85-94, their Holtsnider & Jaffe, 2007:358-359). All the forms of controls are implemented to prevent and respond to the devastating loss or unavailability of IS resources (Hayden, 2010:17).

The proposed IS security e-competencies development framework in this research (Figure 7.2) is an example of a proactive measure that is intended to create a readiness state among the end users in dealing with IS security threats.

This research acknowledges the existence and implementation of security controls such as physical controls, access controls, as well as communication controls such as security guards, walls and fences, password antivirus, firewalls, intrusion detection systems, etc. (Rainer & Cegielski (2013:85-94). However, end users are still the greatest vulnerability (Thomson & von Solms, 2006) against the protection of IS resources. In many organisations (including HEIs), end users are not trained and integrated in the IS security programme of the organisation. This is alongside the weaknesses of security technologies in safeguarding IS resources against social engineering, errors due to lack of skills, improper training, and human hacking (Okenyi & Owens, 2007; Colwill, 2009).

Hence, the protection of IS resources require more than security technologies, but also the education of end users on the features of IS security such as the four spheres of ICT security (policies, technologies, culture, and the environment – both internal and external). Tshinu et *al*. (2014) introduce a proper categorisation of IS resources and end users, as well as assigning appropriate methods of supplying IS security e-competencies to accommodate the needs of HEIs and their context. These elements were included in the proposed IS security e-competencies development framework which was designed by following the requirements of competencies framework development for the HEIs context. All this was done in a way to ensure the IS security e-competencies are supplied to end users at the right level and for the right purpose.

7.8 CHAPTER SUMMARY

The IS security e-competencies development (human aspect of IS security) plays a critical role in the security of IS resources in the HEI environment just as in any other business organisation. From the logging into critical applications and the updating of the antivirus software on a personal computer at home or at work to the handling of critical information in both printed or soft copies and reporting security threats, end users have a critical role to play in the protection of IS resources in their proximate and extended environment.

The non-development of IS security e-competencies of the end users by the four surveyed HEIs implies that these institutions do not understand the importance of end users in the security of IS resources and rely on security technology to protect their IS resources. In this regard, these institutions ignore that the biggest and permanent threat to their IS resources is their internal staff members (end users of IS resources). In this ignorance these institutions put their critical information, their image and reputation, and also the information of their business partners at risk. For example, they are handled by end users who do not have appropriate security competencies to protect them.

Even though HEIs are not financial institutions (as it is echoed during the interviews), it does not mean that there are no information and other IS resources that are critical to the operations of HEIs for which the end users need to be trained for. In fact, with the pervasiveness and reliance on IS resources by HEIs for administration, research, teaching and learning, the enactment of POPI act by South African government, and the reporting on questionable university degrees scandals, the development of IS security e-competencies among the end users in the HEIs environment is of great value.

The IS security e-competency development framework and its supporting frameworks presented in this chapter present a positive step toward a holistic approach to understand and supply IS security e-competencies to end users in the HEI environment. Furthermore, the development of IS security e-competencies among the end users can serve as a supporting mechanism to strengthening the

HEIs' resistance to external IS threats that affect IS resources. However, it also strengthen the resistance to internal threats caused by end users either due to human errors and lack of IS security e-competencies or malicious or intentional acts if they are unaware of the consequences.

From the framework perspective, it can be concluded that the development of IS security e-competencies among the end users flows from the university council strategies and support. Then they are developed on the basis of ICT security frameworks and best practices. Competencies are highlighted in ICT security policies and legal requirements. Thereafter, the competencies are supplied according to the levels of end users and the jobs they occupy, which are linked to the appropriate delivery methods. The development of these IS security e-competencies are therefore an important part of the security programme of the HEIs as their negligence may lead to the ineffective security of IS resources.

To ensure success with the developed model, there is a need of synergy between the various stakeholders within the higher education institution. Mainly, the support and strategic direction from the council, the training and development department of human resources, the legal department to clarify the requirements of the legal Acts, the finance department, the ICT security experts, and the involvement of end users in the supply side as described in the Activity Theory model.

CHAPTER EIGHT: CONCLUSION AND RECOMMENDATIONS

8.1 INTRODUCTION

This chapter starts with revisiting research objectives, continues with a brief overview of the reviewed literature, used research methodology and empirical findings. This is followed by the practical recommendations for development of IS security e-competencies, acknowledgements of contributions and limitations of this study and suggestions for further research in this area of academic investigation. The chapter concludes with a section summary.

8.2 MEETING RESEARCH OBJECTIVES

The Higher Education Institutions (HEIs) environment is a complex environment especially when it comes to the coordination of IS activities and managing their security. On the one hand, the HEI is an open environment in which learning is encouraged and students have to learn how the computer viruses work. On the other hand the security of these IS resources need to be ensured. Hence, the two main objectives of this research were:

- To explore the IS security e-competencies development practices of the four HEIs in the Western Cape Province, and
- To develop a conceptual framework under which the IS security e-competencies are identified and can also effectively be supplied to the end users considering the challenges found in the HEI environment.

The exploration of IS security e-competencies development practices of the four HEIs in the Western Cape Province showed that these HEIs did not formally develop the IS security e-competencies of their end users. They also did not train their end users in order to protect the institutional IS resources. Hence, for the IS security e-competencies development to be effective, this research proposed an IS security e-competencies development framework that can be used in the HEI environment.

To ensure that the presented objectives were manageable, they were subdivided in three sub-objectives of which each were connected to the established research sub-

questions that were formulated to answer the main research question: "*What IS security e-competencies are needed in Higher Education Institution (HEI) environment for effective protection of IS resources and how can these security e-competencies be supplied to IS resources end users?".*

The three research sub-objectives were formulated as follows:

Sub-objective 1: The exploration of the importance of IS resources and their security in the HEI environment. This research sub-objective was successfully achieved through the interviews and the survey questionnaires distributed to the end users as discussed in Chapter 6. The summary of the responses from the interviews revealed that, HEIs increasingly rely on IS resources for almost all their operations; from admission to communication with students to graduation, from administration to research, teaching and learning. Hence, IS resources are now core to the operations of HEIs.

Sub-objective 2: The exploration of IS security e-competencies development "best" practices and how they are currently practiced by the participating HEIs. This sub-objective was achieved by asking questions to participants through interviews and survey questionnaires, which were distributed to the end users. The summary of the answers from the survey interviews revealed that currently the four participating HEIs do not have formal IS security e-competencies development activities for their end users. Yet, the end users are considered as an important part of ICT security programme.

Sub-objective 3: The exploration of optimal ways to supply the needed IS security e-competencies in the HE environment. This sub-objective was also achieved by the exploration of previous publications ("best practice"), asking questions during the interviews, and the completion of the research survey by the end users. The summary of data collected revealed that, in following the principles of competency framework development, it was important to group the end users according to their levels of competencies requirements. In that regard, this research identified three levels of end users: (i) Level 1, which includes all the general end users and general administrative and academic staff members, (ii) Level 2, which includes information

managers and departmental officers, and (iii) Level 3, comprising information curators and/or functional managers.

A mixture of two training methods that are formally integrated in the practices such as contact and online methods, need to be applied to ensure that the end users who cannot attend the contact mode can be reached through the online method or continue the contact mode discussion to online.

Completing these three research objective tasks, the researcher constructed the IS security e-competencies development framework as presented in Figure 7.2.

8.3 OVERVIEW OF LITERATURE REVIEW

Given the complexity of this research topic and the influence that other fields of studies have on it, the achievement of this study's objectives was possible by drawing on the insights from other composite fields and a combination of two approaches to research in the form of a mixed research methodology. In this regard, the literature study was extensively covered in three chapters (Chapters 2, 3, and 4) which were subsequently used to support the empirical findings discussed in Chapters 6, 7, and 8.

Chapter 2 reports on the reviewed literature on the theoretical framework that was used to study the interplay of different artefacts in order to make the supply of IS security e-competencies possible. Notably, the general perspective on various theories was reviewed. This was followed by the literature review on the Activity Theory (AT). In summary, this chapter suggests that the successful development of IS security e-competencies is dependent on the successful identification and categorisation of end users, the tools needed for the development of competencies, the supporting rules, the community, and proper distribution of roles and responsibilities among the participants to the activity system.

Chapter 3 brought the exploration of the field of IS security by highlighting the criteria of information and the importance of information and IS resources security. The common threats to IS resources and related security measures were discussed as

well as the security standards, security culture, and legal requirements from the South African perspective. This chapter provided the foundation for discovering the threats that IS resources face in the HEI environment and the possible security controls that end users need in order to prevent or alleviate these threats.

Chapter 4 is dedicated to the literature review on the competencies frameworks that were used as foundation for developing this research's IS security e-competency framework. It also reported on educational methods for supplying IS security e-competencies in the HEI environment.

The chapter helped in discussing and discovering the levels of IS security e-competencies, and the process for developing an appropriate framework. This included activities such as the identification of the purpose of the framework, categorisation of end users, identification of the source of framework, identification of competencies, and the development of the actual framework such as the one presented in Figure 7.2. In addition, Chapter 4 presents the reviewed literature on training regarding Information and IS security e-competencies development. The literature on the importance of training and options for IS security e-competencies development revealed that it is important to combine different methods for supplying IS security e-competencies in order to ensure that end users with different learning challenges and requirements are accommodated.

The last chapters (Chapters 7 and 8) used the literature review findings to support (or otherwise) the IS security e-competencies development practices as discovered through interviews and survey in the four participating HEIs that participated in this study.

8.4 OVERVIEW OF EMPIRICAL RESEARCH DESIGN

Granted the complexity of the research topic and the need to broaden the respondents' base and obtain the view from the ICT security experts from each of the four participating HEIs as well as from another seven South African HEIs; this research applied a mixed research methodology which helped in combining quantitative and qualitative research methods to collect data from a broader

participants base from various institutional units and backgrounds (ICT, legal, training and development, executives such as registrars, and general end users).

Specifically, using the in-depth interview technique, a number of experts were interviewed from the participating HEIs, including the IS security representatives, the training and development departments, the university council representatives (registrars), and the legal services representatives. In addition, a questionnaire was completed by 385 participants who represented the ICT resources end users. The use of the two data collection techniques (interviews and questionnaires) was in line with the requirements of the mixed research method and helped in broadening the data collection from both ICT security experts and non-experts. In addition, given the participation of the four HEIs in this research, a multiple case study was used as strategy to explore the ICT security e-competencies development practices in-depth. This broad access to participants helped also in addressing a bias regarding the research findings.

8.5 SUMMARY OF DATA ANALYSIS AND RESULTS

The collection and analysis of empirical data for this research was done in phases for the reason of ensuring that data from one phase inform the succeeding phase.

The first phase involved the interaction (through in-depth interviews) with IS security technicians, researchers and academics who have experience in the research topic and have published on the related research topics. It was done in order to obtain their views on the importance of this research and the aspects of IS security e-competencies that need to be developed in the end users of IS resources.

The second phase involved in-depth interviewing of the participants from the four participating HEIs in order to discuss the IS security e-competencies development practices in their respective HEIs. During these interviews, the IS resources end users were identified and sampled for the distribution of research questionnaires.

The third phase was the distribution of the research questionnaires to the sampled end users who voluntarily accepted to participate in this research. A total of 385

questionnaires were successfully completed and returned to the researcher. It also might be useful to report that some end users immediately completed and returned the questionnaire, while others completed theirs after two to five days and e-mailed the researcher a scanned copy. Others were collected from participants' offices. This ensured a high number of valid survey responses.

Where possible, the analysis and discussion of quantitative empirical data was done immediately after the discussion of the qualitative empirical data in order to provide a supporting evidence of the IS security development practices of the participating HEIs as experienced by the end users.

The findings of this research were grouped into two categories:

1. The first category asserted to understand that the IS security e-competencies are not only needed by ICT security experts, but by all the end users who access any form of IS resources in the HEI environment. It was also found that the four participating HEIs did not have a formal framework or process for identifying, categorising, and supplying IS security e-competencies to end users.
2. The second category asserted that the existing ICT skills frameworks such as SFIA, e-CF, and INCOSE that were reviewed in this research focuses only on the assessment of IS security e-competencies of ICT security experts. Hence, this research proposed a framework (Figure 7.2) which can be used for the assessment and supply of IS security e-competencies for end users in the HEI environment. However, the model can also be adapted for business organisations in other industries.

8.6 CONTRIBUTIONS OF THE STUDY

Benefiting from the participation of the four major HEIs in the Western Cape (multiple cases) and the use of different techniques for data collection and analysis, and also good participation from both ICT security experts (in-depth knowledge through in-depth interviews) and end users of IS resources (broad knowledge through questionnaires), this research's contribution to the further development of the IS security knowledge base can be summarised as following.

Through the Activity Theory (AT), this research has been able to discover that the IS security e-competencies development does not happen in isolation. It is a result of interplay between various artefacts in the HEI and support from the entire system. Other theories such as attribution theory, diffusion of innovation, social capital theory, and self-efficiency theory could not demonstrate the interplay between the various components of systems in achieving the object IS security e-competencies development in the HEIs as good as AT. The use of AT as the research theoretical approach demonstrated that if there is an inconsistency and insufficiency in any of the constructs such as ICT security policies, human and financial resources, and the application of security standards or support from management (tools) as is the current status, the outcome of an activity becomes impossible to achieve. Therefore, a successful development of end users' IS security e-competencies (the object of the activity system) depend on:

- The proper identification and categorisation of end users and training instructors (subjects).
- Availability of finances, support from management, workshops and awareness, computing resources and training materials (tools).
- Availability of supporting rules such as ICT security policies, supportive HR policies and security standards (Rules).
- The availability of the HEI community in general, ICT security experts, support staff, and end users who are willing to take the IS security e-competencies development challenge (Community).
- Proper allocation of work and separation of duties between the end users and instructors (subdivision of labour).

In general, the application of Activity Theory (AT) in this study has shown that the success in the development of IS security e-competencies is possible only if the artefacts of the activity system are available in good quantity and quality, and interplay well between each other when needed.

The developed general IS security e-competencies framework has enriched the literature not only in IS security, but also in the theory of human capital development. This can be used to identify specific and general competencies related to IS

resources security that can be included in activities such as the creation and updating of jobs descriptions, training and development, recruitment and selection of employees for certain positions, and the creation of success planning (Gayeski et *al*., 2007).

Furthermore, this study has contributed to emerging knowledge because of its uniqueness in addressing the IS security e-competencies of the end users of IS resources which have been neglected by the previous IT competency frameworks such as Skills Framework for Information Age (SFIA) and European e-Competence Framework (e-CF). The frameworks (SFIA and e-CF) address IT competencies but only for IT professionals. Given that end users are also important in the protection of information and IS resources that process information, they need also to be formally considered in the evaluation and supply of needed IS security e-competencies. Therefore, the importance of IS security e-competencies development frameworks and its related framework which were not provided before.

Practically, this research has found that as employees move from one job to another within the same organisation (to another extend from one organisation to another), they tend to lose the acquired competencies (Schulz, 2013) The IS security e-competencies development framework suggested in this research can be used in HEI and can be adapted by other organisations to develop and manage a stock of auditable IS security e-competencies according to identified categories of employees and the way to supply these competencies which allow the maximum participation.

HEIs are complex organisations and present challenges that are different to other business organisations. The management of IS security is also a complex undertaking and requires a holistic approach. The IS security e-competencies development framework (Figure 7.2) and its supporting Activity Theory framework (Figure 7.1) present the components and that which need to be considered for the successful implementation of IS security e-competencies development in the HEI environment.

In addition to the IS security e-competencies relevant for end users, the framework clarifies also the importance of grouping end users according to their levels, and supporting tools and frameworks to be users, and also the appropriate methods for supplying the identified competencies to enable the HEIs to reach large number of end users. All these can be achieved only if the challenges identified in this research such as the setting of direction and support from all levels of management and provision of resources are addressed.

The model in Figure 7.2 can be used to guide practical development of IS security e-competencies to the end users of IS resources in the HEIs. It can also be used by organisations in other industries.

8.7 LIMITATIONS OF THE STUDY

This study used the multiple case study research design strategy through which the IS security e-competencies development practices of the four HEIs in the Western Cape Province in South Africa that officially participated to this research were thoroughly investigated. The four cases, therefore, can be seen as having limited generalisation to the researched HEIs. This, however, does not mean that the findings of this research cannot be applicable to other South African HEIs since nine ICT security experts from other seven South African HEIs also participated in this study and gave their experience and views on IS security e-competencies and some practices in their HEI environment.

Another limitation was on the limited sample of end users who were drawn only from three HEIs instead of four. One HEI, the HEI04, could not allow the researcher to distribute the questionnaires to the end users because the IS security information needed from end users has been judged by its ethical community as critical. The specific institution had to prevent the leaking of critical information. In the fourth institution, only the interviews were conducted with executives representing the council, the training and development department, and IT security representatives.

Concluding this section on the study limitations, it has to be stated that these limitations did not influence the validity of this study. The results of this study were validated through various means, including the continuous comparison of research empirical data from the interviews with the questionnaires both from a different set of participants. Also, the interview data and findings were validated by the participants and peers who were knowledgeable about the research topic before their final publication. In addition, the results of this research were presented and published in the peer-reviewed international conferences proceedings.

8.8 RECOMMENDATIONS

As discussed throughout this research, information (and the IS resources that collect, store, process, and distribute the information) are considered as lifeblood of any organisation. This means that the protection of the information and the IS resources means protecting the life and the image of the organisation as well. With reference to the protection of the information, it was discovered also in the literature that the ICT security technologies are not effective in protecting the information and other IS resources. There is a need to associate end users' security e-competencies to the security technologies as no security is implemented without human intervention.

For this research, the non-development of IS security e-competencies of end users poses a problem not only to the end users themselves, but also to the entire operation. Especially with the enactment of the South African POPI and other related acts, the non-development of IS security e-competencies for end users means that they become a threat to IS resources, to the organisation, and to each other.

In relation to this research, the following section recommends actions to address the IS security e-competencies development practices of the four participating HEIs.

8.8.1 University Council and executive leadership on IS security e-competencies development

The university council and Senate through their ICT audit committee and the university's IT management department should strive to set the direction and support the development of IS security e-competencies of each employee in each of the participating HEI. The best place to set this direction is through the ICT security policy which must not only be acknowledged through posting them online, but should be enforced by ensuring that employees read, understand the content of the ICT security policy, and also sign it to accept the consequence of their actions if they breach its rules. The King Report III supports this recommendation and suggests that IT governance (including security) is the responsibility of the board of directors (Steenkamp, 2011). In the HEI environment this board is represented by the university council.

8.8.2 IS security e-competencies practices and ICT security policy

The ICT security policy or any of its supporting policies on IS security e-competencies should make clear that the IS security e-competencies should be developed according to the end users' job description and category level. In addition, the end users need to be informed during the first training about their responsibilities in the protection of ICT resources, the procedures for reporting the security threats, and a specific office or ICT security representative that need to be contacted in case of IS threats to ensure that the case of emergency receives the highest priority.

The ICT security policy needs to be enacted. This means that the ICT policy should not only be a document drafted and uploaded on the institution's online presentation for the staff members to access when needed. It must be given to all employees from the first week of employment (Gollmann, 2011:15) to remind them about the importance of ICT security: what is expected from them, and which processes they should follow in case of events such as unsolicited e-mails and during active security threat. The policy needs to be reviewed during the induction week and throughout the security events during the year.

The ICT security policy serves to inform the end users about their responsibilities in relation to IS resources that they access (including Internet and e-mail), to prevent misuse and reduce exposure and legal liabilities (Turban & Volonino, 2012:131). In this ICT security policy or its supporting policies, there is also a need to identify, categorise, and prioritise the information and other IS security resources for appropriate archiving, access, and protection. The end users of IS resources need to be informed about this categorisation. Otherwise, end users can be vulnerable to IS threats and other attacks if they are not made aware of the company's ICT policy and best use practices (Farn et *al*., 2008; Harwood, 2011:117).

8.8.3 The challenge in the supply of IS security e-competencies

The lack of resources as expressed by participants, especially the limited budget and shortage of human resources from both the ICT security department and training and development need to be addressed before the formal implementation of the IS security e-competencies development programme. Of most importance among the resources is the IS security coordinator (or IS security officer), who need to be employed and tasked to coordinate the security activities from both the technology and end users' perspectives.

8.8.4 The supply of IS security e-competencies

Once the IS security e-competencies development programme is officially introduced in the HEI, the institution needs to formally start with the IS security e-competencies development during the induction of new employees. The induction training needs to be a formal class contact mode in which the end users are given the opportunity read, understand, and sign the ICT security policy document. Then the end users need to be engaged at the beginning of each semester with an online security scenario before they can access the network, and then ensure that there is a regular update through newsletters, e-mails, and monthly special events that are included on the calendar.

In addition to the class mode method, the participating HEIs need to formally integrate the online method of delivery for training. The supply of this online training need to meet the requirements of material design and ensure that there is an

interaction between the participant and the trainer. The integration of the two modes needs to be formal and ensure that the end users are given the options before the training. Other modalities should be communicated to them; the combination of different training methods can also ensure that different learning styles are accommodated (Broderick, 2006; Robinson, 2006; Robertson et *al*., 2013).

The institution must also ensure that on promotion of employees, the employees' IS security e-competencies are upgraded to the new employment level. The previous IS security e-competencies are not irrelevant, but they need to be upgraded to the requirement of the new position.

Supplying IS security e-competencies in this way might be a tall order for some HEIs but, according to this study, this would be an appropriate way to make the end users of IS resources, security e-competent.

8.8.5 The use of ICT security framework

The participating (and other) HEIs need also to adopt the best practices presented in the ICT security framework, and use the proposed IS security Figure 7.2 (and its support model Figure 7.1) when implementing the IS security e-competencies development programme. This was developed by following the guidelines of the competencies framework development and was developed on the basis of HEIs' challenges and conditions. The applications of the "best practices" demonstrate the HEIs' commitment to secure and sound business practices (Siponen & Willison, 2009).

The recommended framework plays a role of IS security e-competencies inventory that are auditable according to the category of level of employees in the HEIs. This could help to avoid the loss of skills (Schulz, 2013) when employees move from one position to another within the same HEI or across various HEIs.

8.9 RECOMMENDATIONS FOR FUTURE RESEARCH

This research addressed the development of IS security e-competencies framework that can be used for the development of IS security e-competencies of end users in

the HEIs environment. It focused on the identification, categorisation, and the supply of IS security e-competencies for end users in the HEIs. Due to this research's limited scope, it was not possible to explore in detail other useful constructs that have an impact on the delivery of IS security e-competencies in the HEIs setting such the culture, the enforcement practices, and the implication of legal requirement.

Therefore, future studies in this field can be conducted to address the following:

- The creation of IS security culture that enforce the IS security e-competencies development in the HEI environment.
- The influence of the top management behaviour on the development of end users' IS security e-competencies.
- The adaption of the proposed IS security e-competencies framework for different industry such as the financial industry.
- The comparison of the IS security e-competencies development practices of HEIs to those of other complex organisations such as banking and insurance companies.

8.10 CHAPTER SUMMARY

This study has revealed some elements of inconsistency in the understanding and practices of IS security e-competencies development for the end users of IS resources in the HEI environment. Even though the four HEIs that participated in this study considered that IS resources and the information they produce are core and critical to their operations, and they (participating HEIs) and the reviewed literature recognise that end users of IS resources form a critical part of IS security programme, they failed to develop the IS security e-competencies of their end users of IS resources.

Adding to the above problem is the fact that the governing body or the council of the four HEIs that participated to this research or their respective ICT management and audit committees failed to provide the direction through their ICT security policies or the supporting policies on how to address the IS security e-competencies development of their end users. At the same time putting at risk their reputation, their valuable information (and the IS resources) and those of their business partners and

stakeholders like pharmaceutical companies, military organisations, and the business organisations that fund research projects in the HEIs at the mercy of uninformed end users who may voluntarily or involuntarily or inappropriately act against the information they come across.

Moreover, in the absence of formal IS security e-competencies development and the non-inclusion of end users into the IS security programme of the four HEIs, it can be said that these HEIs focus their IS security efforts and funding on the ICT security technologies. According to the literature, the security technologies are not highly effective in securing the IS resources against the external threats. The reason for this is that internal users have full knowledge of the security technology measures and therefore, can easily bypass them. In relation to end users, if they involuntarily and carelessly mishandle information and IS resources, if they cannot properly manage their login details and not log-off after accessing critical systems, these actions may lead to unauthorised access of institutions' critical systems. The security technologies do not effectively provide for such kind of threats to IS security.

Beside the carelessness and involuntary threats from the end users, the literature and the ICT security experts from the four participating HEIs recognise that the internal threats to information and IS resources outweigh those from the external environment. Still, the four participating HEIs concentrate their ICT security efforts and funding more on security technologies than on human measures. As an example, it was discovered that the four participating HEIs distributed their ICT security policies only by uploading it on their internal online system, and the majority of end users never accessed or read it, which means they are not informed of its content.

This research therefore suggests the IS security e-competencies framework with its competencies, the supply methods, and other components that need to be considered for a formal development of end users of IS security e-competencies as a holistic approach to IS resources security in the complex HEI environment.

This research endeavoured to support the need for the protection of information and related IS resources in the HEI or in any other organisation. Also, that this is not a reserved premise of the ICT security experts and the application of technological controls. It is an obligation of everyone employed in the institution despite their position in the organisation.

REFERENCES

Abdullah, Z. (2014). Activity Theory as analytical tool: A case study of developing student teachers' creativity in design [Online]. Procedia – Social and Behavioural Sciences, Vol. 131 (May, 2014), 70-84.

Abdulrazeg, A.A., Norwawi, N. & Bazi, N. (2012) Security measurement based on GQM to improve application security during requirements stage [Online]. International Journal of Cyber-security and digital forensics, Vol. 1 (3), 211-220.

Acevedo, E.O. (ed.). (2012). The Oxford Handbook of Exercise Psychology. U.S.A: Oxford University Press.

Agrawal, A. & Khan, R.A. Securo-Phobia: A New challenge to usage of security technologies [Online]. Journal of Software Engineering and Simulation, Vol. 2, Issue 1 (2014), 1-3.

Ahlan, A.R. & Lubis, M. (2011). Information security awareness in University: Maintaining learnability, performance, and adaptability through roles of responsibility [Online]. IEEE 7th International Conference on Information Assurance and Security (IAS), (December, 2011). 246-250. doi:10.1109/ISIAS.2011.6122827.

Ala-Mutka, K. (2011). Mapping digital competence: toward a conceptual understanding [Online]. Joint Research Centre (JRC) Technical notes, (2011). Available from: http://ftp.jrc.es/EURdoc/JRC67075_TN.pdf [Accessed: 10 November 2014].

Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study [Online]. Computers & Security, Vol. 29 (4), 432-445.

Albrechtsen, E. (2007). A qualitative study of users' view on information security [Online]. Computers & security, Vol. 26 (4), 276-289.

Alfawaz, S., Nelson, K. & Mohannak, K. (2010). Information security culture: A behavior compliance conceptual framework [Online]. Proceedings of 8th Australasian Information Security Conference (AISC), (2010), 47-55.

Allen, D., Karanasios, S. & Slavova, M. (2011). Working with Activity Theory: context, technology, and information behaviour [Online]. Journal of the American Society for Information Science and Technology, 62 (4), 776-788.

Allen, H.W. (2010). Language-Learning motivation during short-term abroad: an activity theory perspective [Online]. Foreign language annals, Vol. 43 (1), 27-49.

Ardalan, K. (2010). Globalization and finance: four paradigmatic views [Online]. Journal of globalization studies. Vol. 1 (2), 41-67.

Ardoin, N.M., DiGiano, M., Bundy, J., Chang, S., Holthuis, N. & O'Connor, K. (2014). Using digital photography and journaling in evaluation of field-based environmental education programs [Online]. Studies in Educational Evaluation, 41 (2014), 68-76.

Armstrong, M. & Taylor, S. (2014). Armstrong's handbook of human resources management practice. 13th edition. United Kingdom: Kogan Page.

Arthur, J., Waring, M., Coe, R. & Hedges, L.V. (eds.). (2012). Research methods and methodologies in education. London: Sage.

Asgrahani, M. & Shankararaman, V. (2014). Skills Frameworks: A tool for reform in information technology higher education [Online]. IEEE 9th International Conference on Computer Science & Education (ICCSE), (Vancouver, 2014).

Ash, D. (2014). Positioning Informal Learning Research in Museums within Activity Theory: From theory to practice and back again [Online]. Curator the Museum Journal, Vol. 57(1), 107-118.

Ashenden, D. (2008). Information security management: A human challenge? [Online]. Information Security Technical Report, Vol. 13 (4), 195-201.

Avison, D. & Pries-Heje, J. (eds.). (2005). Research in information systems: A handbook for research supervisors and their students. Great Britain: Elsevier.

Axelrod, C.W., Bayuk, J.L., & Schutzer, D. (eds.). (2009). Enterprise information security and privacy. London: Artech House.

Baartman, L.K.J. & de Bruijn, E. (2011). Integrating knowledge, skills and attitudes: conceptualising learning processes toward vocational competence [Online]. Educational Research Review, Vol. 6 (2), 125-134.

Babbie, E. (2007). The practice of social research. International Student Edition. 11th edition. International student edition. U.S.A: Thomson

Babbie, E. (2008). The basics of social research. 4th edition. International student edition. U.S.A: Thomson

Baltzan, P. & Phillips, A. (2010). Business driven technology. 4th Ed. U.S.A: McGraw-Hill.

Banga, G., Crosby, S. & Pratt, I. (2014). Trustworthy computing for the cloud-Mobile Era: A leap forward in systems architecture [Online]. IEEE Consumer Electronics Magazine, Vol. 4 (3), 31-39.

Beisse, F. (2004). A Guide to Computer User Support for Help Desk and Support Specialists. 3rd Edition. U.S.A: Cengage learning.

Beisse, F. (2010). A Guide to Computer User Support for Help Desk and Support Specialists. International edition. 4th edition. U.S.A: Cengage learning.

Beisse, F. (2013). A Guide to Computer User Support for Help Desk and Support Specialists, International Edition. 5rd edition. U.S.A: Cengage learning.

Beqiri, E. (2010). ICT and e-learning literacy as an important component for the new competency-based curriculum framework in Kosovo [Online]. Journal Research in Educational Sciences, Vol. 1 (1), 7-21.

Berragan, L. (2013). Conceptualising learning through simulation: an expansive approach for professional and personal learning [Online]. Nurse Education in Practice, 13 (4) 250-255.

Bharosa, N., Lee, J., Janssen, M. & Rao, H.R. (2012). An activity theory analysis of boundary objects in cross-border information systems development for disaster management [Online]. Security Informatics, 15 (1), 1-17.

Bickman, L. & Rog, D.J. (2009). The SAGE handbook of applied social research methods. 2nd edition. U.S.A: Sage publications.

Blanche, M.T., Durrheim, K., & Painter, D. (eds.). (2006). Research in practice: Applied methods for the social sciences. Cape Town: University of Cape Town Press.

Bless, C. & Higson-Smith, C. (2004). Fundamentals of social research method: an African perspective. 3rd Edition. Cape Town: Juta.

Booth, A.L. & Katic, P. (2011). Men at work in a Land Down-Under: Testing some predictions of human capital theory [Online]. British Journal of Industrial Relations, 49 (1), 1-24.

Börner, R., Moormann, J. & Wang, M. (2012). Staff training for business process improvement: the befit of role-plays in the case of KreditSim [Online]. Journal of Workplace Learning, Vol. 24, (3), 200-225.

Boshoff, R. & van Niekerk, J. (2009). E-mail security awareness at Nelson Mandela Metropolitan University (registrar's division) [Online]. Proceedings of the Information Security South Africa (ISSA) Conference, (2009), 279-291.

Bosworth, S., Kabay, M.E. & Whyne, E. (eds.). (2009). Computer security handbook, 5th edition. U.S.A: Wiley.

Brandén, M. (2013). Couples' Education and regional mobility – the importance of Occupational Income and Gender [Online]. Population, Space, and Place, 19 (5), 522-536.

Broderick, J.S. (2006). ISMS, security standards and security regulations [Online]. Information security technical report, Vol. 11 (1) 26 – 31.

Bryant, A. & Charmaz, K. (eds.). (2007). The SAGE Handbook of Grounded Theory: Paperback Edition. London: Sage Publications.

Bryman, A. & Buchanan, D. (eds.). (2009). The Sage Handbook of Organizational Research Methods. London: Sage Publications.

Buecker, A. (2007). Understanding SOA security design and implementation. IBM Redbooks.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. Management Information Systems (MIS) Quarterly, Vol. 34 (3), 523-548.

Burrel, G. & Morgan, G. (1979). Sociological paradigms and organizational analysis: elements of the sociology of corporate life. Portsmouth: Heinemann.

Calder, A. (2005). A business guide to information security. United Kingdome: Kogan Page.

Calder, A. (2013). The case for ISO27001:2013. 2nd Edition. United Kingdom: IT Governance Publishing.

Card, N.A. (2012). Applied meta-analysis for social science research. New York: Guilford Press.

Charmaz, K., (2006). C*onstructing Grounded Theory: A Practical Guide Through Qualitative Analysis*, C.A.: Sage, Thousand Oaks

Chang, S.H., Chen, D.F. & Wu, T.C. (2012). Developing a competency model for safety professionals: Correlations between competency and safety functions. Journal of Safety Research, Volume 43, (5–6), 339-350.

Chen, J.C. & Martin, A. R. (2015). Role-Play Simulations as a Transformative Methodology in Environmental Education [Online]. Journal of Transformative Education, Vol. 13 (1), 85-102.

Chen, W., Lai, M.M., Li, T.C., Chen, P.J., Chan, C.Y. (2011). Professional development in enhanced by serving as a mini-CEX preceptor [Online]. Journal of continuing education in the health professions, Vol. 31, (4), 225-230.

Ciampa, M. (2014). Security Awareness: Applying practical security in your world. 4th edition. International edition. U.S.A: Cengage.

Clarke, R. (2005). *Situational Analysis: Grounded theory after the postmodern turn*, C.A.: Sage, Thousand Oaks

Clarke, P.A.J. & Fournillier, J.B. (2012). Action research, pedagogy, and activity theory: Tools facilitating two instructors interpretations of the professional development of four preservice teachers. [Online]. Teaching and Teacher Education, 28 (5), 649-660.

Cohen, L., Manion, L. & Marrison, K. (2011). Research methods in education. 7th Edition. Oxford: Routledge.

Colwill, C. (2009). Human factors in information security: the insider threat – who can you trust these days? [Online]. Information Security Technical Report, Vol. 14 (4), 186-196.

Cooper, D.R. & Schindler, P.S. (2006). Business research methods. 9th edition. Singapore: McGraw-Hill.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap [Online]. Computers in Human Behavior, 28 (5), 1849-1858.

Cragg, P., Caldeira, M. & Ward, J. (2011). Organisational information systems competences in small and medium-sized enterprises [Online]. Information & Management, Vol. 48 (8), 353-363.

Cresswell, J. W. (1998). Qualitative Inquiry and Research Design: Choosing Among Five Traditions, London: Sage

Creswell, J.W. (2003). Research design: qualitative, quantitative, and mixed methods approaches. 2nd Ed. U.S.A: Sage Publications.

Creswell, J.W. (2009). Research design: qualitative, quantitative, and mixed methods approaches. 3rd edition. U.S.A: SAGE publications.

Creswell, J.W. (2012). Educational research: planning, conducting, and evaluating quantitative and qualitative research. International edition. 4th edition. Boston: Pearson.

Creswell, J.W., Clark, V.L.P. (eds.). (2011). Designing and Conducting Mixed Methods Research. 2nd edition. U.S.A: SAGE publications.

Crocker, A. & Eckardt, R. (2013). A multilevel investigation of individual- and unit-level Human Capital Complementarities [Online]. Journal of Management, Vol. 40 (2), 509-530.

Crook, T.R., Todd, S.Y., Combs, J.G., Woehr, D.J. & Ketchen, D.J., Jr. (2011). Does human capital matter? A meta-analysis of the relationship between human capital and human performance [Online]. Journal of Applied Psychology, Vol. 96 (3), 443-456.

D'Arcy, J. & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance [Online]. Information Management & Computer Security, Vol. 22 (5), 474-489.

Daft, R.L., Murphy, J. & Willmott, H. (2010). Organization theory and design. Singapore: Cengage Learning.

De Chesnay, M. (ed.). (2015). Nursing Research Using Grounded Theory: Qualitative Designs and Methods in Nursing. U.S.A: Springer Publishing.

De Vos, A., & Fouche, C. (1998). General Introduction to Research Design, Data Collection Methods and Data Analysis. In D. V. (ed), Research at Grassroots: A primer for caring professions. Pretoria: Van Schaik Publishers.

De Vaus, D.A. (2001). *Research Design in Social Research*, London: Sage.

De Win, B., Scandariato, R., Buyens, K., Grégoire, J. & Joosen, W. (2009). On the secure software development process: CLASP, SDL, and Touchpoints compared [Online]. Information and Software Technology. Vol. 51 (7), 1152-1171.

Department of Higher Education and Training (DHET) (2012). Green paper for Post-school education and training [Online]. Available from: http://www.che.ac.za/sites/default/files/publications/DHET_green_paper_post_school_education_training.pdf [Accessed: 15 October 2014].

Dey, I, (1999). *Grounding grounded theory: guidelines for qualitative inquiry*. San Diego: Academic Press.

Dhillon, G. (2007). *Principles of information systems security: text and cases*. U.S.A: Wiley.

Doherty, N.F., Anastasakis, L. & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of universities policies [Online]. International Journal of Information Management, Vol. 29 (6), 449-457.

Dooley, L. M. (2002). Case Study Research and Theory Building, *Advances in Developing Human Resources*, Vol. 4, No. 3. pp. 335-354.

Dohesty, N.F., Anastasakis, L. & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy [Online]. *International Journal of Information Management*, Vol. 31 (3), 201-209.

Draganidis, F. & Mentzas, G. (2006). Competency based management: A review of systems and approaches [Online]. Information Management & Computer Security, Vol. 14 (1), 51-64.

Dunn, D.S. (2010). The practical researcher: a student guide to conducting psychological research. 2nd edition. Singapore: Wiley-Blackwell.

Eikebrokk, T.R. & Olsen, D.H. (2007). An empirical investigation of competency factors affecting e-business success in European SMEs [Online]. Information and management, Vol. 44 (4), 364-383.

Eminağaoğlu, M. Uçar, E. & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study [Online]. Information security technical report, Vol. 14 (4), 223-229.

Engeström, Y. (2001). Expensive learning at work: Toward an activity theoretical reconceptualization [Online]. Journal of Education and work, Vol. 14 (1), 133-156.

Engeström, Y. (2011). From design experiments to formative interventions [Online]. Theory & Psychology, Vol. 5 (21), 598-628.

Enqeström, Y (2001) Expansive learning at work: Toward an activity theoretical reconceptualization. Journal of Education and work, Vol. 14 (1), 133-156.

European Committee for Standardization (CEN). (2014a). European e-Competence Framework 3.0 [Online]. Available from: http://www.ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf [Accessed: 15 November 2014].

European Committee for Standardization (CEN). (2014b). Building the e-CF – a combination of sound methodology and expert contribution 3.0 [Online]. Available from: http://www.ecompetences.eu/wp-content/uploads/2014/02/Methodology_documentation_e-CF_3.0_CEN_CWA_16234-3_2014.pdf [Accessed: 15 November 2014].

European Committee for Standardization (CEN). (2014c). European e-Competence Framework 3.0: User guide for the application of the European e-Competence framework 3.0 [Online]. Available from: http://www.ecompetences.eu/wp-content/uploads/2014/02/User-guide-for-the-application-of-the-e-CF-3.0_CEN_CWA_16234-2_2014.pdf [Accessed: 15 November 2014].

Fakeh, S.K.W., Zulhemay, M.N., Shahibi, M.S., Ali, J. & Zaini, M.K. (2012). Information security awareness amongst academic librarians [Online]. Journal of Applied Sciences Research, 8 (3), 1723-1735.

Farn, K.J., Lin, S.K., & Lo C.C. (2008). A study on e-Taiwan information system security classification and implementation [Online]. Computer Standards & Interfaces, Vol. 30 (1-2), 1-7.

Flick, U. (2011). Introducing research methodology: a beginner's guide to doing a research project. London: Sage publications.

Fourie, H., Plant, K., Coetzee, G.P. & van Staden, J.M. (2013). Internal audit competencies: skills requirements for internal audit management in South Africa [Online]. Southern Journal of Accountability and Auditing Research, Vol. 15 (2013), 75-85.

Furnell, S. & Moore, L. (2014). Security literacy: the missing link in today's online society? [Online]. Computer Fraud & Security, Vol. 2014 (5), 12-18.

Furnell, S. & Rajendran, A. (2012). Understanding the influences on information security behaviour [Online]. Computer fraud and security, Vol. 2012 (3), 12-15.

Furnell, S.M. (2009). The irreversible march of technology [Online]. Information Security Technical Report, Vol. 14 (4), 176-180.

Gable, G. G. (1994). Integrating case study and survey research methods, an example in information systems, *European Journal of Information Systems*, Vol. 3, No. 2, pp. 112-126.

Gamerschlag, R. (2013). Value relevance of human capital information [Online]. Journal of Intellectual Capital, Vol. 14 (2), 325-345.

Gayeski, D.M., Golden, T.P., Andrade, S. & Mason, H. (2007). Bringing competency analysis into the 21st century [Online]. Performance Improvement, Vol. 46 (7), 9-16.

Gilbert, N. (2008). Researching social life. 3rd Edition. Great Britain: Sage Publications.

Gimmon, E. & Jonathan, L. (2010). Founder's human capital, investment, and the survival of new high-technology ventures [Online]. Research Policy, 39 (2010) 1214-1226.

Gollmann, D. (2011). Computer security. 3rd edition. United Kingdom: John Wiley.

Goodson, P. (2010). Theory in health promotion research and practice: Thinking outside the box. U.S.A: Jones and Barlett Publishers.

Gorman, G.E. & Corbitt, B.F. (2002). Core competencies in information management education [Online]. New Library World, Vol. 103 (11-12), 436-445.

Gray, D.E. (2009). Doing research in the real world. Great Britain: Sage Publications.

Gray, D.E. (2014). Doing research in the real world. Great Britain: Sage Publications.

Grealish, L. & Smale, L.A. (2011). Theory before practice: implicit assumptions about clinical nursing education in Australia as revealed through a shared critical reflection [Online]. Contemporary nurse: A Journal for Australian Nursing Profession, Vol. 39 (1), 51-64.

Greasley, P. (2008). Quantitative data analysis using SPSS: An introduction for Health & Social Science. Glasgow: Open University Press.

Greenfield, T. (ed.). (2002). Research methods for postgraduates. 2nd Edition. Great Britain: Arnold.

Guasch, T., Alvarez, I. & Aspasa, A. (2010). University teacher competencies in a virtual teaching/learning environment: Analysis of a teacher training experience [Online]. Teaching and Teacher Education, Vol. 26 (2), 199-206.

Guo, K.H. & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model [Online]. Information & Management, Vol. 49 (6), 320-326.

Hamond, M. & Wellington, J. (2013). Research Methods: The Key Concepts. New York: Routledge.

Hans, K. (2010). Cutting edge practices for secure software engineering [Online]. International Journal of Computer Science and Security (IJCS), Vol. 4 (4), 403-408.

Haralambos, M. & Holborn,M. (1991). Sociology: themes and perspectives. 3rd edition. London: Collins Educational.

Hardwood, M. (2011). Security strategies in Web Applications and social networking. U.S.A: Jones & Barlett Learning.

Harwood, M. (2011). Security strategies in Web applications and social networking. U.S.A: Jones & Bartlett learning.

Hasan, H. & Pfaff, C.C. (2012). An activity theory analysis of corporate wikis [Online]. Information Technology & People, Vol. 25 (4), 423-437.

Hawkes, C.L. & Weathington, B.L. (2014). Competency-based versus job description: effects on applicant attraction [Online]. Institute of Behavioural and Applied Management. Available from: http://www.ibam.com/pubs/jbam/articles/vol15/No3/article%205%20Final%20Weathington%20Competency%20vs%20Task%20Based%20Job%20Descriptions%20after%20asst%20editor.pdf [Accessed: 12 December 2014].

Hayden, J. (2014). Introduction to health behavior theory. 2nd edition. U.S.A: Jones & Bartlett Learning.

Hayden, L. (2010). IT security metrics: A practical framework for measuring security and protecting data. U.S.A: McGraw-Hill.

Heather, J. (2004). Skills unlocked [Online]. Training: ProQuest Educational Journals, Vol. 41 (11), 39-40.

Henn, M., Weistein, M. & Foard, N. (2006). A Short introduction to social research. Great Britain: Sage Publications.

Henn, M., Weistein, M. & Foard, N. (2009). A critical introduction to social research. 2nd edition. United Kingdom: Sage Publications.

Hennink, M., Hutter, I. & Bailey, A., (2011). Qualitative research methods. Great Britain: Sage Publications.

Herath, T. & Rao, H.R. (2009). Encouraging security behaviours in organisations: role of penalties, pressures and perceived effectiveness [Online]. Decision Support Systems, Vol. 47 (2), 154-165.

Herath, T. & Roa, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations [Online]. European Journal of information systems, (2009) 18, 106-125.

Hesse-Biber, S.N. (2010). Mixed Methods Research: Merging Theory with Practice. U.S.A: Guilford Press.

Higher Education and Training Laws Amendment Act 23 of 2012. Government Gazette. Vol. 570. 36022 of 19 December 2012. Cape Town: Republic of South Africa.

Holt, J. & Perry, S.A. (2011). A pragmatic guide to competency: Tools, frameworks and assessment. U.K: British Computer Society (BCS).

Holtsnider, B. & Jaffe, B. (2007). IT Manager's handbook: getting your new job done. 2nd edition. U.S.A: Morgan Kaufmann.

Hon, A.H.Y. (2012). When competency-based pay relates to creative performance: The moderating role of employee psychological need [Online]. International Journal of Hospitality Management, Vol. 31 (1), 130-138.

HORNBY, A.S. (2000). Oxford Advanced Learner's Dictionary of current English. 6th Edition. China: Oxford University Press.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management [Online]. Information security technical report, Vol. 13 (4), 247-255.

Information Resources Management Association (ed.). (2012). Machine Learning: Concepts, Methodologies, Tools and Applications: Concepts, Methodologies, tools and applications. U.S.A: IGI Global.

International Journal of Human-Computer studies. (2007). Information security in the knowledge economy [Online]. The International Journal of Human-Computer studies, Vol. 65 (1), 1-2.

IT Governance Institute, ITGI. (2007). COBIT 4.1. U.S.A: ISACA.

Jankowicz, A.D. (2005). Business research projects. 4th Edition. Italy: Thomson Learning.

Johassen, D. & Land, S. (eds.). (2012). Theoretical foundations of learning environments. 2nd Edition. U.S.A: Routledge.

Johl, C., von Solms, R, & Flowerday, S. (2013). Information Technology governance process maturity in Higher Education Institutions in South Africa [Online]. South African Journal of Higher Education, Vol. 27 (3), 627-644.

Johnson, E.C. (2006). Security awareness: switch to a better programme [Online]. Network security, Vol. 2006, (2). 15-18.

Johnson, R.B. & Onwuegbuzie, A.T. (2004). Mixed methods research: a research paradigm whose time has come. American Educational Research Association, [Online]. Vol. 33 (7), 14-26.

Jones, A. (2009). How do you make information security user friendly? [Online]. Information security technical report, Vol. 14 (4), 213-216.

Jones, A. (2010). How do you make information security user friendly? [Online]. Information security technical report, Vol. 14 (4), 213-216.

Jones, O. & Holt, R. (2008). The creation and evolution of new business ventures: an activity theory perspective [Online]. Journal of Small Business and Enterprise Development, Vol. 15 (1), 51-73.

Kaml, G., Weiss, C.C., Dezendorf, P., Ishida, M., Rice, D.H., Klein, R. & Salfinger, Y. (2014). Developing a competency framework for U.S. State food and feed testing laboratory personnel [Online]. Journal of AOAC International, Vol. 97 (3), 768-772.

Karjaleinen, M. & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches [Online]. Journal of the Association for Information Systems, Vol. 12 (8), 518-555.

Kasser, J., Frank, M. & Zhao, Y.Y. (2010). Assessing the competencies of systems engineers [Online]. 7th Bi-annual European Systems Engineering Conference (EuSEC), (2010), 1-9.

Kasser, J., Hitchins, D., Frank, M. & Zhao, Y.Y. (2012). A framework for benchmarking competency assessment models [Online]. Systems engineering, Vol. 16 (1), 29-44.

Keith, M. Shao, B. & Steinbart, P.J. (2007). The usability of passphrases for authentication: an empirical study [Online]. International Journal of Human-Computer Studies, Vol. 65 (1), 17-28.

Kim, Y. & Park, H. (2014). An investigation of the competencies required of airline cabin crew members: the case of a Korean Airline [Online]. Journal of Human Resources in Hospitality & Tourism, Vol. 13 (1), 34-62.

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, J. (2008). Security considerations in the system development life cycle [Online]. U.S.

Department of Commerce: National Institute of Standards and Technology (NIST). Available from: http://delivery.acm.org/10.1145/2210000/2206279/SP800-64-Revision2.pdf?ip=146.232.0.1&id=2206279&acc=OPEN&key=646D7B17E601A2A5%2EC011CE1E941E2524%2E4D4702B0C3E38B35%2E6D218144511F3437&CFID=618530383&CFTOKEN=19820353&__acm__=1421331129_0f0b54f6524d45dbcf633b223ac8fb72 [Accessed: 23 November 2014].

Knights, D. & Willmott, H. (eds.). (2012). Introducing organizational behaviour and management. 2nd Edition. United Kingdom: Cengage Learning.

Kouns, J. & Minoli, D. (2010). Information technology risk management in enterprise environments: A review of industry practices and a practical guide to risk management teams. U.S.A.: John Wiley & Sons.

Kreuh, N. (ed.) (2012). Bulletin: The way towards e-competency [Online]. E-Education Bulleting. Available from: http://www.sio.si/fileadmin/dokumenti/bilteni/E-solstvo_BILTEN_ANG_2012_screen.pdf [Accessed: 25 April 2013].

Kumar, R. (2011). Research Methodology: A Step-by-Step Guide for Beginners. 3rd Edition, London: Sage publications.

Lapan, S.D. & Quartaroli, M.Q. (eds.). (2009). Research essentials: and introduction to designs and practices. San Francisco: Jossey-Bass.

Law, P. (2010). Gaming outcome of accountants and human capital theory: Macau evidence [Online]. Management Research Review, Vol. 33 (12), 1174-1186.

Leach, J. (2003). Improving user security behaviour [Online]. Computers & Security, Vol. 22 (8), 685-692.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. & Breitner, M.H. (2014). Information security awareness and behaviour: a theory-based literature review [Online]. Management Research Review, Vol. 37 (12), 1049-1092.

Liaw, S.S., Hatala, M. & Huang, H.M. (2010). Investigating acceptance toward mobile learning to assist individual knowledge management: Based on activity theory approach [Online]. Computers & Education, 54, 446-454.

Lichtman, M. (2010). Qualitative research in education: A user guide. 2nd Edition. U.S.A: Sage Publications.

Lucas, M. (2012). IT skills Gap forces CIOs to get creative [Online]. Computerworld. Available from: http://www.computerworld.com/article/2502591/it-careers/it-skills-gap-forces-cios-to-get-creative.html [Accessed: 10 December 2012].

Lynn, A. (2009). Security training 101: how to create an effective end user security awareness programme [Online]. Network World, Vol. 26. (16), 30.

Marcinkowski, S.J. & Stanton, J.M. (2003). Motivational aspects of information security policies [Online]. IEEE international conference on systems man and cybermetrics, Vol. 3 (2003), 2527-2532.

Maree, K. & van der Vesthuizen, C. (2009). Head start in designing proposals in the social sciences. Cape Town: Juta.

Maree, K. (ed.). (2007). First steps in research. Pretoria: Van Schaik.

Martin, B.C., McNally, J.J. & Kay, M.J. (2013). Examining the formation of human capital in entrepreneurship: A meta-analysis of entrepreneurship education outcomes [Online]. Journal of Business Venturing, 28 (2), 211-224.

Martin, N. & Imboden, T.R. (2014). Information security and insider threats in small medical practices [Online]. Twentieth Americas Conference on Information Systems, Savannah, (2014), 1-9.

Maxwell, J. A. (2008). Designing a qualitative study. Available from: http://www.corwin.com/upm-data/23772_Ch7.pdf [Accessed 8 May 2012]

McCaston, K. (2005) Tips for Collecting, Reviewing, and Analyzing Secondary Data, available from: http://pqdl.care.org/Practice/DME%20-%20Tips%20for%20Collecting,%20Reviewing%20and%20Analyzing%20Secondary%20Data.pdf [Accessed 20 June 2013]

Miettinen, R., Paavola, S. & Pohjola, P. (2012). From habituality to change: contribution of Activity Theory and Pragmatism to Practice Theories [Online]. Journal for the Theory of social Behaviour, Vol. 42 (3), 345-360.

Miller, R.L. & Brewer, J.D. (eds.) (2003). The A-Z of social research. London: SAGE Publications.

Milne, J.A. (2005). IT security samurai [Online]. ProQuest, Network Computing, Vol. 16 (21), 55-60.

Mitrovic, Z. (2008). A theoretical framework for the adequacy of electronic small business development services, Doctoral Theses, Cape Peninsula University of Technology, unpublished.

Monk, E. F. & Wagner, B. J. (2009). Concepts of Enterprise Resource planning, 3rd Edition. U.S.A: Cengage Learning.

Monk, E.F. & Wagner, B.J. (2013). Concepts of Enterprise Resource planning, 4th Edition. U.S.A: Cengage Learning.

Morelock, R. (2012). Help your franchisees implement training programmes that engage their employees [Online]. Franchising world, June (2012). Available from: http://www.franchise.org//IFA_NEWS/Help_Your_Franchisees_Implement_Training_Programs_That_Engage_Their_Employees/ [accessed: 23 November 2013].

Munro, M.C., Huff, S.L., Marcolin, B.L. & Compeau, D.R. (1997). Understanding and measuring user competence [Online]. Information & Management, Vol. 33 (1), 45-57.

Murphy, G.T., MacKenzie, A., Alder, R., Langley, J., Hickey, M. & Cook, A. (2012). Pilot-testing an applied competency-based approach to health human resources planning [Online]. Health Policy and Planning, (December, 2012), 1-11.

Myers, M.D. (1997). Qualitative research in information systems. Management Information Systems Quarterly (MISQ), Vol. 21 (2), 241-242.

Nardi, B.A. (ed.). (1996). Context and conciousness: Activity Theory and human-computer Interaction. U.S.A: Massachusetts Institute of Technology.

National Qualification Framework Act, Nº 67 of 2008. Government Gazette Vol. 524 (31909). 17 February 2009. Cape Town: Government Printer.

National Qualifications Framework Act, No. 67 of 2008. Articulation Policy. Government Gazette Nº 37775. 27 June 2014.

Ng, T.W.H. & Feldman, D.C. (2010). Human capital and objective indicators of career success: The mediating effects of cognitive ability and conscientiousness [Online]. Journal of Occupational and Organisational Psychology, 83 (1), 207-235.

Nieto-Montenegro, S.J.L, Brown, & Laborde, L.F. (2006). Using the health action model to plan food safety educational materials for Hispanic workers in the mushroom industry [Online]. Food Control, Vol. 17 (10), 757-767.

Okenyi, P.O. & Owens, T.J. (2007). On the anatomy of human hacking [Online]. Information Systems Security, Vol. 16 (6) 302-314.

Olivier, M.S. (2004). Information technology research: a practical guide for computer science and informatics. 2nd edition. Pretoria: Van Schaik Publishers.

Ornes, L.L. & Gassert, C. (2007). Computer competencies in a BSN program [Online]. Research briefs. 46 (2), 75-78.

Orsoni, A. & Colaco, B. (2013). A competency framework for software development organisations [Online]. IEEE 15th International Conference on Computer Modelling and Simulation, (2013), 507-511.

Oz, E. & Jones, A., (2008). Management information systems. United Kingdom: Cengage Learning.

Padayachee, K. (2012). Taxonomy of compliant information security behavior [Online]. Computer security, Vol. 31, (5), 673-680.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employee's behaviour towards IS security policy compliance [Online]. IEEE Proceedings of the 40th international conference on systems sciences (HICSS), (2007). DOI:10.1109/HICSS.2007.206.

Paraskeva, F., Mysirlaki, S. & Papagianni, A. (2010). Multiplayer online games as educational tools: Facing a new challenges in learning [Online]. Computer & Education, Vol. 54 (2), 498-505.

Park, S., Cho, Y., Yoon, S.W. & Han, H. (2013) Comparing team learning approaches through the lens of activity theory, [Online]. European Journal of Training and Development, Vol. 37 (9), 788-810.

Pascal, J. & Brown, G. Ontology, Epistemology and Methodology for Teaching Research Methods. In: Garner, M., Wagner, C. & Kawulich, B. (eds.). (2009). Teaching research methods in the social science. England: Ashgate Publishing.

Peña-Ayala, A., Sossa, H. & Méndez, I. (2014). Activity theory as a framework for building adaptive e-learning systems: A case to provide empirical evidence [Online]. Computers in Human Behavior, Vol. 30 (January, 2014), 131-145.

Peng, M. & Meyer, K. (2011). International Business. Singapore: Cengage Learning.

Pettenger, M., West, D. & Young, N. (2014). Assessing the impact of role play simulation on learning in Canadian and US classrooms [Online]. International Studies Perspectives, 15 (4), 491-508.

Petty N.J. Thomson, O.P. and Stew, G. (2012). Ready for a paradigm shift? Part 1: Introducing the philosophy of qualitative research [Online]. Manual Therapy, 17 (4), 267-274.

Piccoli, G. 2012. Essentials of Information Systems for Managers. U.S.A: John Wiley.

Prasolova-Førland, E., Fominykh, M., Darisino, R. & Mørch, A.I (2013). Training Cultural Awareness in Military Operations in a Virtual Afghan Village: A Methodology for Scenario Development [Online]. 46th Hawaii International Conference on System Sciences, (2013), 903-912.

Preston, B. & Kennedy, K. (1995). The national competency framework for beginning teaching: a radical approach to initial teacher education? [Online]. Australian Educational Researcher Volume, Vol. 22 (2), 27-62.

Punch, K.F. (2009). Introduction to Research Methods in Educations. London: Sage Publications.

Punch, K.F. (2014). Introduction to Social Research: Quantitative and Qualitative Approaches. London: Sage Publications.

Qian, Y., Fang, Y. & Gonzalez, J.J. (2012). Managing information security risks during new technology adoption [Online]. Computers & security, 31 (8), 859-869.

Rainer Jr, R.K. & Cegielski, C.G. (2013). Introduction to information systems: international student version. 4th edition. Singapore: John Wiley.

Rajas-Muslera, R., Urquiza, A. & Cepeda, I. (2011). Competency-Based model through IT: an action research project [Online]. Systemic Practice and Action Research, 25 (2), 117-135.

Ramesh, I.V. & Glass, R.L. (2002). Research in information systems: an empirical study of diversity in the discipline and its journals [Online]. Journal of Management Information Systems. [Online]. Vol. 19 (2), 129-174.

Rastogi, R. & von Solmons, R. (2012). Information security service culture – information security for end-users [Online]. Journal of Universal Computer Science, Vol. 18, (12), 1628-1642.

Rauch, A. & Rijsdijk, S.A. (2011). The effects of general and specific human capital on long-term growth and failure of newly founded business [Online]. Entrepreneurship Theory and Practice, Vol. 37 (4), 923-941.

Rauch, A., Frese, A. & Utsch, A. (2005). Effect of human capital and long-term human resources development and utilisation on employment growth of small-scale businesses: a causal analysis [Online]. Entrepreneurship Theory and Practice, Vol. 29 (6), 681-698.

Ravotto, P. Competence-based learning in Europe & the SLOOP2DESC model [Online]. In: Fulantelli, G. & Oprea, L. (eds.). (2011). Preparing the teachers for a competence-based education system [Online]. Sharing Learning objects in an open perspective to develop European skills competence (Sloop2desc), (2011). Available from: http://www.adam-europe.eu/prj/5936/prj/Sloop2desc_book.pdf [Accessed: 23 August 2014].

Rehman, A., Alqahtani, S., Altameen, A. & Saba, T. (2014). Virtual machine security challenges: Case studies [Online]. International Journal of Machine Learning & Cybernetics, Vol. 5 (5), 729-742.

Rehman, S. & Mustafa, K. (2009). Research on Software Design Level Security Vulnerabilities [Online]. ACM SIGSOFT Software Engineering Notes, Vol.36 (6), 1-5.

Reid, A.M. (2012). The role of the 'Practice Trainer" as an agent of co-configuration in supporting professional learning [Online]. White Rose Research Online, 2012. Available from: http://eprints.whiterose.ac.uk/77739/3/reidam1.pdf [Accessed: 11 June 2014].

Rezgui, Y. & Marks, A. 2008. Information security awareness in higher education: an exploratory study [Online]. Computers & Security, Vol. 27 (7-8), 241-253.

Rhee, H.S., Kim, C. & Ryu, Y.U. (2009). Self-efficacy in information security: its influence on the users' information security practice behavior [Online]. Computers & Security, Vol. 28 (8), 816-826.

Rhee, H.S., Ryu, Y.U. & Kim, C.T. (2012). Unrealistic optimism on information security management [Online]. Computers & Security, 31 (2), 221-232.

Richard, A.E., Brown, J.L., Radhakrishna, E.P., Nieto-Montenegro, S. & Cutter, C.N. (2013). Development and implementation of a "Counter-Top" Training Programme to increase retention of food safety knowledge, alter behaviour, improve attitude and increase skills of Spanish-speaking retail employees [Online]. Food Protection Trends, Vol. 33 (1), 10-19.

Rob, P., Coronel, C., & Crockett, K. (2008). Database systems: Design, Implementation & Management. International Edition. London: Cengage Learning.

Robertson, L.A, Boyer, R.R, Chapman, B.J. & Eifert, J.D. (2013). Educational needs assessment and practices for grocery store food handlers through survey and observation data collection [Online]. Food control 34 (2), 707-703.

Robinson, B. (2006). Security training no longer on the backburner [Online]. Federal Computer Week. Available from: http://fcw.com/Articles/2006/10/02/Security-training-no-longer-on-the-back-burner.aspx [Accessed: 12 March 2014].

Rospigliosi, A.P., Greener, S., Bourner, T. & Sheehan, M. (2013). Human capital or signaling, unpacking the graduate premium [Online]. International Journal of Social Economics, Vol. 41 (5), 420-432.

Ruzek, J.I., Rosen, R.C., Marceau, L., Marceuu, L., Larson, J.M., Garvert, D.W., Smith, L. & Stoddards, A. (2012). Online Self-administered training for post-traumatic stress disorder treatment providers: design and methods for a randomized, prospective intervention study [Online]. Implementation Science, 7 (43), 1-14.

Sabeil, E., Manaf, A.B.A., Ismail, Z. & Abas, M. (2011). Cyber forensic competency-based framework – A review [Online]. International Journal on New Computer Architecture and their Application (UNCAA), Vol. 1 (3), 991-1000.

Sahinidis, A.G. & Bouris, J. (2008). Employees training effectiveness relationship to employee attitudes [Online]. Journal of European Industrial Training, Vol. 32 (1), 63-76.

Sahu, P.K. (2013). Research Methodology: A Guide for Researchers in Agricultural Science, Social Science and Other Related Fields. India: Springer.

Salas, E., Wildman, J.L. & Piccolo, R.F. (2009). Using simulation-based training to enhance management education [Online]. The academy of Management Learning and Education, Vol. 8 (4), 559-573.

Saldana, J. 2009. The coding manual for qualitative researchers. London: Sage publications.

Saldaña-Ramos, J., Sanz-Esteban, A., García, J. & Amescua, A. (2014). Skills and abilities for working in a global software development team: a competence model [Online]. Journal of Software: Evolution and Process, 26 (3), 329-338.

Sanchez, J.I. & Levine, E.L. (2009). What is (or should be) the difference between competency modeling and traditional job analysis? Human resources management review, 19 (2), 53-65.

Sarkar, K.R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures [Online]. Information security technical report, Vol. 15 (3), 112-133.

Sattarova, N.I. (2013). Information Security of knowledge economy students [Online]. Middle-East Journal of Scientific Research, Vol. 18 (8), 1199-1203.

Schermerhon, Jr. J.R., Osborn, R.N., Uhl-Bien, M. & Hunt, J.G. (2012). Organizational behaviour. 12th edition. International student version. Asia: Wiley.

Schermerhorn, J.R., Osborn, R.N., Uhl-Bien, M. & Hunt, J.G. (2012). Organisational behaviour. 12th Edition, International student version. Asia: Wiley.

Schulz, E., Chowdhury, S. & van De Voort, D. (2013). Firm productivity moderated link between human capital and compensation: the significance of task-specific human capital [Online]. Human Resource Management, Vol. 52 (3), 423-439.

Schwalbe, K. (2014). Managing Information Technology Projects. 7th International Edition. U.S.A: Cengage Learning.

Sedinić, I., Lovrić, Z. & Perušić, T. (2014). Customer and user education as a tool to increase security level [Online]. 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), (May, 2014), 1441-1445.

Shahri, A.B., Ismail, Z. & Rahim, N.Z.A. (2013). Security culture and security awareness as the basic factors for security effectiveness in Health Information Systems [Online]. Jurnal Teknologi, 64, (2), 7-12.

Shankar, D., Agrawal, M. & Rao, H.R. Emergency response to Mumbai Terror Attacks: An Activity Theory Analysis. In: Santanam, R., Sethumadhavan, M. & Virendra, M. (2011). Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives. U.S.A: IGI Global.

Shelly, G. B., & Rosenblatt, H. J. (2010). Systems Analysis and Design. 8th Ed. Canada: Cengage Learning.

Shkedi, A. (ed.). (2005). Multiple Case Narrative: A Qualitative Approach to Studying Multiple Populations. Philadelphia: Johan Benjamins Publishing.

Singh, G., Hawkins, L. & Whymark, G. (2009). Collaborative knowledge building process: an activity theory analysis [Online]. The Journal of information and Knowledge Management Systems, Vol. 39 (3), 223-241.

Siponen, M.T. (2000). A conceptual foundation for organisational information security awareness [Online]. Information Management & Computer Security, 8 (1), 31-41.

Siponen, M.T. (2000). Critical analysis of different approaches to minimizing user-related faults in information systems security: Implications for research and practice [Online]. Information Management & Computer Security Vol. 8 (5), 197-209.

Siyahhan, S., Barab, S.A. & Downton, Michael, P. (2010). Using activity theory to understand intergenerational play: The case of Family Quest [Online]. Computer-Supported Collaborative Learning, Vol. 5 (4), 415-432.

Skills Development Amendment Act, No. 31 of 2003. Government Gazette. Vol. 461 (25720). 14 November 2003. Cape Town: Government Printer.

Slater, M. & Lally, V. (2013). The realities of researching alongside virtual youth in late modernity creative practices and activity theory [Online]. Journal of Youth Studies, Vol. 17 (1), 1-25.

Smit, P.J., Cronje, G.J., Brevis, T. & Vrba, M.J. (2011). Management principles: A contemporary edition for Africa. 5th Edition. Juta: Cape Town.

Smith, A.D. (2004). E-security issues and policy development in an international-sharing and networked environment [Online]. New Information Perspectives, Vol. 56 (5), 272-285.

Smith, M. (2009). Changing staff behaviour [Online]. Information security technical report, Vol. 14 (4), 175.

Somekh, B. & Lewin, C. (eds.). (2005). Research Methods in the Social Sciences. Great Britain: Sage Publications.

Someth, B. & Lewin, C. (eds.). (2006). Research methods in the social sciences. London: Sage Publications.

Spais, G.S. (2010). Search Engine Optimisation (SEO) as a dynamic online promotion technique: the implications of activity theory for promotion managers [Online]. Innovative Marketing, Vol.6 (1), 7-24.

Stander, A., Dunnet, A. & Rizzo, J. (2009). A survey of computer crime and security in South Africa [Online]. Proceeding of Information Security South Africa (ISSA), (2009), 217-226.

Stanton, J.M., Stam, , K.R. Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviour [Online]. Computers & Security, Vol. 24 (2), 124-133.

Stokoe, E. Simulated interaction and communication skills training: The conversation-analytic role-play method. In Antaki, C. (ed.). (2011). Applied conversation analysis: Intervention and Change in Institutional Talk. United Kingdom: Palgrave Macmillan.

Stuart, K. (2014). Activity theory as a reflective and analytic tool for action research on multi-professional collaborative practice [Online]. Reflective Practice, Vol. 15 (3), 347-362.

Succar, B., Sher, W. & Williams, A. (2013). An integrated approach to BIM competency assessment, acquisition and application [Online]. Automation in construction, Vol. 35 (November, 2013), 174-189.

Suh, E., West, J.J. & Shin J. (2012). Important competency requirements for managers in the hospitality industry [Online]. Journal of hospitality, leisure, sport & tourism education, 11 (2), 101-112.

Sun, J. & Qu, Z. (2014). Understanding health information technology adoption: A synthesis of literature from an activity perspective [Online]. Information Systems Frontiers. (2004). DOI 10.1007/s10796-014-9497-2.

Susanto, H., Almunawar, M.N., & Tuan, Y.C. (2011). Information security management systems standards: A comparative study of the big five [Online]. International Journal of Electrical & Computer Science (IJECS-IJENS). Vol. 11 (5), 21-27.

Tamjidyamcholo, A., Bin Baba, M.S., Gholipour, R. & Yamchello, H.T. (2013). Information security professional perception of knowledge-sharing intention in virtual communities under social cognitive theory [Online]. 3rd International Conference on Research and Innovation in Information Systems, ICRIIS' 13 (2013).

Tashakkori, A. & Teddlie, C. (eds.). (2003). Handbook of mixed methods in social & behavioral research. U.S.A: Sage publications.

Tashakkori, A. & Teddlie, C. (eds.). (2010). SAGE handbook of mixed methods in social & behavioral research. U.S.A: Sage publications.

Teddlie, C. & Tashkkori, A. (2009). Foundations of mixed methods research: integrating quantitative and qualitative approaches in the social and behavioural sciences. U.S.A: Sage publications.

The SFIA Foundation. (2011). SFIA 5 framework reference. [Online]. Available at: http://www.sfia-online.org/v501/en/publications/reference-guide/at_download/file.pdf [Accessed 20 May 2013].

The SFIA Foundation. (2011). SFIA 5 framework reference: skills defined in categories and subcategories [Online]. Available from: https://www.sfia-online.org/v501/en/publications/reference-guide/at_download/file.pdf [Accessed: 15 November 2014].

Theoharidou, M., Tsalis, N. & Gritzalis, D. (2014). Smart Home Solutions: Privacy Issues. In: van Hoof, J., Demiris, G. & Wouters, E.J.M. (2015). Handbook of Smart Homes, Health Care and Well-Being. Switzerland: Springer Publishing.

Thiadens, T. (2005). Manage IT: organising IT demand and IT supply. The Netherlands: Springer Publishing.

Thomson, K.L. & von Solms, R. (2006). Towards an information security competence maturity model [Online]. Computer fraud & security, Vol. 2006 (5), 11-15.

Thomson, K.L., von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture [Online]. Computer fraud & security, Vol. 2006 (10), 7-11.

Time, M. (2011). Social research: Issues, methods and process. 4th Edition. New York: McGraw-Hill Education.

Timmis, S. (2014). The dialectical potential of Cultural Historical Activity Theory for researching sustainable CSCL practices [Online]. Computer-Supported Collaborative Learning, Vol. 9 (1), 7-32.

Tippins, M.J. & Sohi, R.S. (2003). IT competency and firm performance: IS organisational learning a missing link [Online]. Strategic Management Journal, Vol. 24 (8), 745-761.

Tolnai, A. & von Solms, S. (2009). Solving security issues using information security awareness portal [Online]. International Conference for Internet Technology and Secured Transactions (ICITST), (2009), 1-5.

Topchyan, T.R. (2014). Engineering Competence Frameworks and Topic Modelling [Online]. Mathematical Problems of Computer Science, Vol. 41, 55-62.

Trafford, V. & Leshem, S. (2008). Stepping stones to achieving your doctorate. London: McGraw-Hill.

Tripathi, K. & Agrawal, M. (2014). Competency based management in organisational context: a literature review [Online]. Global Journal of Finance and Management, Vol. 6 (4), 349-356.

Tshinu, M.S., Mitrovic, Z. & Twum-Darko, M. (2014). CD-ROM. Security e-competencies: the spheres and levels in the higher education environment of South Africa [Online]. Proceedings of 5th International Conference on Education and Information Management (ICEIM-2014), 324-331.

Tsohou, A., Karyda, M. & Kokolakis, S. (2012). Analyzing trajectories of information security awareness [Online]. Information security awareness, Vol. 25 (3), 327-352.

Turban, E. & Volonino, L. (2012). Information Technology for management. International student version. 8th Edition. Asia: John Wiley & Sons.

Turban, E., & Rainer Jr, R.K. (2009). Information Systems: Enabling and transforming business. 2nd Edition. International student version. Asia: John Wiley & Sons.

Turban, E., Rainer Jr, R.K. & Potter, R. (2005). Introduction to information technology. 3rd Edition. U.S.A: John Wiley & Sons.

Unger, J.M., Rauch, A., Frese, M. & Rosenbusch, N. (2011). Human Capital and entrepreneurial success: A meta-analysis review [Online]. Journal of Business Venturing, Vol. 26, (2011) 341-358.

Ungureanu, M. (2013). Information security as part of the overall corporate governance – IT governance [Online]. Centre for European Studies (CES) Working papers, Vol. (2), 300-3010.

Urquhart, C. (2013). Grounded theory for qualitative research: A practical guide. London: Sage Publications.

Vacca, J.R. (ed.). (2009). Computer and information security handbook. U.S.A: Morgan Kaufmann.

van Niekerk, J.F. & von Solms, R. (2010). Information security culture: A management perspective [Online]. Computers & security, Vol. 29 (4), 476-486.

Venkatesh, V. Brown, S.A., & Bala, H., (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. Management Information Systems (MIS) Quarterly, Vol. 37 (1), 21-54.

Verdon, S., McLeod, S. & Wong, S. (2014). Reconceptualizing practice with multilingual children with speech sound disorders: people, practicalities and policy [Online]. International Journal of Language & Communication Disorders, DOI: 10.1111/1460-6984.12112, 1-15.

von Konsky, B.R., Jones, A. & Miller, C. (2013). Embedding professional skills in the ICT curriculum [Online]. Proceedings of 30th Ascilite Conference, (2013), 883-887.

von Solms, R., Thomson, K.L., & Maninjwa, M. (2011). Information security governance control through comprehensive policy architectures [Online]. IEEE Information Security South Africa (ISSA), (2011), 1-6.

Vroom, C. & von Solms, R. (2004). Towards information security behavioural compliance [Online]. Computer & Security, Vol. 23 (3), 191-198.

Wang, V.C.X. & King, K.P. (ed.). (2008). Innovations in Career and Technical Education: Strategic Approaches Towards Workforce Competencies Around the Globe. U.S.A.: Information Age Publishing.

Welman, J.C. & Kruger, S.J. (2001). Research Methodology. 2nd Ed. Cape Town: Oxford University Press.

West, R. & Brown, J. (2013). Theory of addiction. 2nd Edition. United Kingdom: John Wiley.

White, B. (2002). Writing your MBA dissertation. U.K: Thomson.

Whitman, M.E. & Mattord, H.J. (2010). Management of information security. 3rd Edition. International Edition. U.S.A: Cengage.

Whitman, M.E. & Mattord, H.J. (2014). Management of Information Security. 4th Edition. International Edition. U.S.A: Cengage Learning.

Whitman, M.E. (2004). In defense of the realm: understanding the threats to information security [Online]. International Journal of Information Management, Vol. 24 (1), 43-57.

Whitton, N. (2014). Game Theory for Learning & Teaching: Research and Theory. New York: Routledge.

Wiant, T.L. (2005). Information security policy's impact on reporting security incidents [Online]. Computer & Security, Vol. 24 (6), 448-459.

Wilkinson, D. (2004). The CICA's IT Competency model [Online]. International Journal of Accounting Information Systems, Vol. 5 (2) 245-250.

Williams, L.Y. (2012). Keeping infosec a step ahead of the bad guys [Online]. Computer World. Available from: http://www.computerworld.com/article/2497567/security0/how-can-we-keep-infosec-pros-a-step-ahead-of-the-bad-guys-.html [Accessed: 25 November 2014].

Williams, P.A.H. (2007). Medical data security: are you informed or afraid? [Online]. International Journal of Information and Computer Security, Vol. 1 (4), 414-429.

Williams, P.A.H. (2008). In a 'trusting' environment, everyone is responsible for information security [Online]. Information Security Technical Report, Vol. 13 (4), 207-215.

Williman, N. (2005). Your Research Project: A Step-by-Step Guide for the First-Time Researcher. 2nd Edition. London: Sage Publications.

Willis, J.W. (2007). Foundations of qualitative research: interpretive and critical approaches. U.S.A: Sage publications.

Willison, R. & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention [Online]. Communication of the ACM, Vol. 52 (9), 133-137.

Wood, C.C. (1995). Shifting Information Systems Security Responsibility from User Organizations to Vendor/Publisher Organizations [Online]. Computers & Security, Vol. 14 (4), 283-284.

Woon, I.M.Y. & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications [Online]. International Journal of Human-Computer Studies, Vol. 65 (1), 29-41.

Wright, P.M. & McMahan, G.C. (2011). Exploring human capital: putting human back into strategic human resource management [Online]. Human Resource Management Journal, Vol. 21 (2), 93-104.

Yildirim, E.Y., Akalp, G., Aytac, S. & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey [Online]. International Journal of Information Management, Vol. 31 (4), 360-365.

Yoon, C. & Kim, H. (2013). Understanding computer security behavioural intention in the workplace – An empirical study of Korean firms [Online]. Computer security behaviour, Vol. 26, (4), 401-419.

Yoon, C.Y. (2009a). Measures of perceived end-user computing competency in an organisational computing environment [Online]. Knowledge-Based Systems. Vol. 22 (6), 471-476.

Yoon, C.Y. (2009b). The effect factors of end-user task performance in a business environment: focussing on computing competency [Online]. Computer in human behaviour. Vol. 25 (6), 1207-1212.

Zafar, H. (2013). Human resource information systems: Information security concerns for organisations [Online]. Human Resource Management Review, Vol. 23 (1), 105-113.

APPENDICES

Appendix A: UWC ethical clearance

OFFICE OF THE DEAN
DEPARTMENT OF RESEARCH DEVELOPMENT

28 May 2014

To Whom It May Concern

I hereby certify that the Senate Research Committee of the University of the Western Cape approved the methodology and ethics of the following research project by Mr MS Tshinu (Information Systems)

Research Project: A functional-interpretive approach to security e-competency in the higher education institution: A comparative case of four South African higher education institutions in the Western Cape Province.

Registration no: 14/3/26

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

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

Ms Patricia Josias

Research Ethics Committee Officer

University of the Western Cape

Private Bag X17, Bellville 7535, South Africa

T: +27 21 959 2988/2948. F: +27 21 959 3170

E: pjosias@uwc.ac.za www.uwc.ac.za

Appendix B: Steps for designing a competency framework

1. Launching the programme by developing the plan and deciding on the Human Resource (HR) to be followed, the project plan, and the resources and costs.
2. Involving the staff at different level and communicate with them on the process.
3. Designing the framework and its competency list: the core competencies are to be drawn after the interaction of the participating HEIs, their end-users staff members, ISs security experts and their Human Resource Development (HRD) departments of these HEIs. The ICT security experts from other HEIs were also consulted to get their input on needed competencies for end-users.
4. Design the framework and define the competencies: the requirement is that care must be taken to avoid the ambiguity for the required ISs security e-competencies. For this requirement, the competencies have been grouped according to the job levels of end-users identified in the HEI that are also grouped in five categories.
5. Definition of the usage of the framework by selecting the appropriate application of the framework. Which in this research was selected to be used during the induction period for all the new recruited employees, but it can be used also at the beginning of any training organised by the institution to the current employees.
6. Testing of the framework: this test is done during the second interviews with the representatives of participating HEIs.
7. Finalise the frame with the suggestion from the interviews to create the final version of the framework.
8. Communicate the result with the stakeholders.
9. Training of the users and HR staff members or responsible ISs security e-competencies development concerned department in the HEI.
10. Monitor the use of the framework in the institution and evaluate its usage by the institution.

Source: Armstrong & Taylor (2014:91)

Appendix C: Quantitative data analysis research code book in SPSS

ITEM	CODE	Measure
Question Number	Number	Nominal
Higher Education Institution (HEI) Reference	{1, HEI01}, {2, HEI02}, {3, HEI03}	Nominal
Gender	{1, Male}, {2, Female}	Nominal
Age Group	{1, 20yrs and below}, {2, 21-25yrs}, {3, 26-30yrs}, {4, 31-35yrs}, {5, 36-40yrs}, {641-45yrs}, {7, 46-50yrs}, {8, 51-55yrs}, {9, 56-60yrs}, {10, 60yrs and above }	Nominal
Employment status	{1, Contract employment}, {2, Permanent employment}	Nominal
Highest Qualification	{1, Below matric}, {2, Matric}, {3, Diploma or Bachelor}, {4, Honours or Postgraduate}, {5, Mater's}, {6, Doctorate}	Ordinal
Years working for the institution	{1, 20yrs and below}, {2, 2-5yrs}, {3, 5-8yrs}, {4, 8-11yrs}, {5, 11-14yrs}, {6, 14-17yrs}, {7, 17-20yrs}, {8, 20yrs and above}	Nominal
Do you use a computer or laptop to do your work?	{0, No}, {1, Yes}	Nominal
Do you use local intranet to do your work?	{0, No}, {1, Yes}	Nominal
Do you use Internet to do your work?	{0, No}, {1, Yes}	Nominal
Do you use printer and its related services to do your work?	{0, No}, {1, Yes}	Nominal
Other IT resources	None	Nominal
How often have you received	{0, Not often}, {1, Often}	Nominal

suspicious or unwanted e-mails this year?		
Have you attended a formal training on IT security at this institution?	{0, No}, {1, Yes}	Nominal
If yes to the question above, who provided the training to you?	{1, Current employer}, {2, Previous employer}, {3, Own development}, {4, Other}	Nominal
How do you perceive your responsibility in relation to IT resources security?	{0, IT resources security is not my responsibility}, {1, IT resources security is my responsibility}, {2, IT resources security is the responsibility of IT technicians}, {3, It is a shared responsibility between end-users and IT technicians}	Nominal
Do you know where the security features of your computer are located?	{0, No}, {1, Yes}	Nominal
Do you back up the information on your PC on external storage drive?	{0, No}, {1, Daily}, {2, Weekly}, {3, Monthly}, {4, Year}	Nominal
Have you been informed on what to do in case of security threat?	{0, No}, {1,Yes}	Nominal
If yes to previous question, what will you do if unknown user remotely controls your computer (You may select more than one)?	{0, Nothing}, {1, Switch off the computer}, {2, Call technician}, {3, Wait until it is freed}, {4, Switch off and call technicians}, {5, Remove Internet cable}	Nominal
How relevant are the IT security competencies in relation to your work?	{1, Additional work}, {2, Important for me and IT resources}, {3, Irrelevant to me}, {4, No choice}	Nominal
How important is the security of IT resources to you?	{1, I am not sure}, {2, Less important}, {3, Very important}	Nominal

I rely on my computer and other IT resources to do my work	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
A computer and Internet are important IT resources for my job	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know that the institution has an acceptable use policy for IT resources and I have read it	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I have read this institution's IT security policy	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I have been trained on this institution's IT security policy	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know what is allowed and not allowed in term of access to IT resources and the Internet	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know the degree of punishment related to mishandling and inappropriate usage of institutional IT resources	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I have been trained on how to use and maintain security technologies related to IT resources I access	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I can identify different security threats affecting IT resources I have access in my environment	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I have been informed on what to do in case of IT security threat in my environment	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know who to contact in case of IT security related threat	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4,	Ordinal

	Agree}, {5, Strongly agree}	
I know this institution has an established IT security e-competencies development culture	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know the top management and my manager model this institution's IT security e-competencies development culture	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I use my own computer or mobile phone to access e-mails and connect to network off the campus	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know the risks associated with the off campus access to the e-mail and institution's network?	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
I know the legal implications of my actions on IT resources and related security	{1, Strongly disagree}, {2, Disagree}, {3, I do not know, 4, Agree}, {5, Strongly agree}	Ordinal
Would you attend institutional IT security training related to your job level?	{0, No}, {1, Yes}	Nominal
Do you prefer attending classroom (contact) mode?	{0, No}, {1, Yes}	Nominal
Do you prefer online training mode?	{0, No}, {1, Yes}	Nominal
Do you prefer information provided on CD or DVD?	{0, No}, {1, Yes}	Nominal
Do you prefer printed notes for self-reading?	{0, No}, {1, Yes}	Nominal
Other mode	None	Nominal
Reasons for classroom mode	None	Nominal
Reasons for online training mode	None	Nominal
Reasons for CD or DVD mode	None	Nominal
Reasons for printed notes mode	None	Nominal
Question Number	None	Nominal

Appendix D: South African information security Acts

The Protection of Personal Information Act of 2013

The Protection of Personal Information Act, 4 of 2013 (referred to POPI) has been officially signed by the South African president and published (Republic of South Africa, Government Gazette No. 37067, November 2013) as Law in November 2013. It gives all organisations that collect and process personal data of their stakeholders (automated and non-automated intended to form part of filing system) the obligation to ensure that the collected data is protected against any disclosure for other purpose than it was collected for. The Act applies to all organisations operating within the national boarders and the transfer of data outside of the republic.

The key content of the Protection of Personal Information Act, 4 of 2013 related to this research include the following:

- The identification of what constitutes personal information: for the purpose of this Act, any information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person that include the (but not limited) information related to race, gender, sex, pregnancy, marital status, mental health, well-being, disability, religion, conscience, belief, criminal or employment history, integrity number, symbol, e-mail address, telephone number, location, online identifier, education and medical, financial, criminal, employment history, biometric information, personal opinion and preference, name, or other particular assigned to the person.
- The establishment of eight conditions for the lawful processing of personal information by or for responsible party which are:
    - Accountability: the responsible party must comply with the stipulated conditions of the Act at the time of processing.
    - Lawful processing: the personal information needs to be processed in reasonable manner that does not infringe the privacy of data subject.
    - Purpose specification: the processing of personal information is only in accordance with adequate and relevant purpose.
    - Further processing limitation: must be in line with the purpose for which it was collected for.

- Information quality: the responsible party must ensure that the personal information is accurate, complete, not misleading and updated.
- Openness: the documentation related to the processing of personal information under its responsibility and ensure that subject are informed when their personal information are collected.
- Security and safeguarding: the responsible party must ensure that reasonable technical and organisational measures are implemented to prevent loss, damage, or unauthorised access to or processing of personal information. This includes the identification of risks, protection against the identified risks, and the operator is tasked to inform the responsible party (notification of data subject through mail, e-mail, website, publication in the news media as may be directed by the regulator) where there are reasonable grounds to believe that unauthorised access to personal information has occurred.

  The notification of data subject may only be delayed if the public body responsible for the prevention, detection or investigation of offences or the regulator determines that such notification can impede a criminal investigation by the public body concerned.

- Data subject participation: the data subject has the right to access to personal information free of charge after adequate proof of identity and request the records or description of the personal information. In case of payment of fee to access personal information, a written estimate of such fee must be given before the service. In case of refusal to access personal information, such refusal must be in compliance with the Law.

  The data subject may, in the prescribed manner request the correction or deletion of personal under responsible party control if is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.

- Unless the processing of personal information is to comply with the following criteria such as the prohibition on processing of personal information such as religious or philosophical beliefs, race of ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, criminal behaviour, and alleged commission does not apply: when it is collected with the consent of the subject, the defense of a right or obligation in law, to comply with international public law, for historical, statistical, or research purpose to the extent that it is for public interest, information has been deliberately made public by the data subject, or it appears to be impossible to or would involve a disproportionate effort to ask for consent from data subject.

  The regulator may upon the application by a responsible party and by notice in the gazette, authorise the responsible party to process special personal information if such processing is in public interest (national security, prevention, detection and prosecution of offenses, interest of public body, fostering compliance, historical, statistical, research, and freedom of expression) and appropriate measures have been put in place to protect the data subject.

- The breach and unlawful processing of personal information by responsible party may result in fine or imprisonment for a period of up to 10 years or to both a fine and such imprisonment.

The Protection of Personal Information Act comes to strengthen the Bill of Rights promulgated by the South African Constitution which ensures that the individual's right to privacy when the information is processed by responsible party, 'subject to justifiable limitations' (Protection of Personal Information Act, 2013) such as right to access to information free flow of information.

In terms of its application and the promotion of the constitutional Bill of rights and the establishment of regulator body to deal with the issues related to the breach of the

Act, the POPI Act is not applied in isolation. It is also established to promote Access to information Act, 2000 which is also briefly describe in the following section.

The Promotion of Access to Information Act of 2000

As it is with the POPI Act, The Promotion of Access to Information Act, 2 of 2000 was also promulgated by the South African government in February 2000 (Republic of South Africa, Government Gazette No 20852, February 2000) with intention to strengthen the constitutional right (section 32(1)(a) and section 32(1)(h) which pride for everyone's right 'to access any information held by the State' and 'the horizontal application of the right of access to information held by another person to everyone when that information is required for the exercise or protection of any right' respectively) of access to any information (one of IS resources) held by the state, public, and private companies and provide for any other aspect related to the access to information with exception to public bodies and official such as cabinet members, judicial function and courts, individual members of parliament and provincial legislature in their capacity (The Promotion of Access to Information Act of 2000).

The Promotion of Access to Information Act of 2000 provides that:

- The requester must be given the access to information after the compliance with the procedural requirements and reasons to access the information.
- The request can be made to the information officer through his/her address, fax, and e-mail in a prescribe form. The request can also be made orally for individuals who are illiterate.
- The requester must provide sufficient particulars for proper identification.
- The Act provides also for cases such as when the record cannot be found, children under the age of sixteen, and those people who are incapable of managing their affairs.

Apart from its provision for access to information, The Promotion of Access to Information Act of 2000 provides also for mandatory protection of third party who is natural person by refusing access to record if the 'disclosure would involve unreasonable disclosure of personal information about the third party, including the deceased individual'. Apart from the cases where the individual consent was given,

information is ready available to the public, well-being of individual (physical and mental health) under the care of requester, deceased requester's next of skin, and any other form as allowed by the law. In any case, the request that within the 21 days after the request has been received or transferred, the third party must be informed and make representation as to why the access should be refused.

Any other form of request to access information must be refused especially if it is of the nature of violating trade secret and about research being carried out on behalf of the third party or the person carrying the research, financial and scientific damage, information was supplied in confidence, and to prejudice that third party, and if the disclosure can endanger the life and safety of individual, property, affect the management of the economy, and the safety of the public and the Republic.

The Electronic Communications and Transactions Act of 2002

In either teaching and learning or information IS resources are at the centre of HEIs' operations in electronic form and need also to comply with the Electronic Communications and Transactions (ECT) Act, 2002 (Republic of South Africa, Government Gazette No. 23708, 2 August 2002) which regulates the online transactions and communications which could not be well regulated through the common laws applied to offline transactions.

Among the other regulations provided by the ECT Act of 2002 include:

- The recognition of online transaction and its related documents as official transaction with regard to the law. In this regards, the transaction is conducted through data message, which is a data generated in form of voice or online record that can be generated, sent and received between the transacting parties (reasonable party) as long they can interpret and understand the content.

  The exception to this regulation includes the transaction for the sale of immovable property and its lease for twenty years or more (Gereda, 2006), or other transactions which require paper agreement. In the case of requirement for storage and production of transaction document, a data message can be

viewed an original if it fulfils the requirement such as originality and integrity as required by the law. If the certified or registered document is required, a data message that is authenticated by the South Africa Post Office (SAPO) Ltd and sent to the destination e-mail address is sufficient.

- The recognition of online signature, which can be both just electronic signature or advanced electronic signature. Any of these two can be accepted as an official signature in a data message in case there is no specification of the type of signature to be provided in the transaction.

- The recognition of the impact of cybercrime and the appointment of cyber inspectors, these inspectors can among other functions monitor the activities of websites operating in public domain to report unlawful activities.

- Provision for the management of critical databases and their components located in the same or different premises. These databases contain information of nature that can compromise the security of the country, the economic and social well-being of its people. The minister has to recommend to security measures such as their registration, their management (including the protection, technology used to access and archive data, integrity authenticity of the data contained, and physical safety of their managers).

- To protect the consumer against the abuse and the management of cryptography service providers. The Act provides also the option for the consumer to withdraw or cancel the transaction within seven days and be charged only the transport fees to supplier. The unsolicited e-mails must not be considered as a binding agreement if the consumer fails to respond to them, and the later be provide with option to unsubscribe from the list, and also on the request of the consumer how his/her details where obtained.

In general, the ECT Act facilitates and regulates the online transactions and communications by ensuring that the shortcomings rising between the consumers and suppliers of services (in this research represented by students and HEI

respectively) when transactions or agreement (both commercial and non-commercial) are carried online (Gereda, 2006) or dealt with when they arise. The Act ensures also that the electronic transactions conducted in South Africa are in line with international standards and it does not seen as validating any online transaction (Republic of South Africa, Government Gazette No. 23708, 2 August 2002).

Appendix E: Participants profile and response rate

From qualitative data analysis, the participation from the four HEIs in the Western Cape was 100%. This means that all the targeted units of analysis or key stakeholders in the development of IS security e-competencies development participated to the research as demonstrated in the following Table E.1.

Table E.1: Research participants' profile from the four participating HEIs

Higher Education Institutions (HEIs)	DATA COLLECTION TECHNIQUES		
	In-depth interview		Survey questionnaire
	Section	Duration (Hours)	Number of Participants
HEI01	1. Security experts	01:06	154
	2. HR Training and development	01:08	
	3. Registrar office	01:00	
	4. Legal representative office	01:00	
HEI02	1. Security expert	01:50	160
	2. Training and development	01:00	
	3. Registrar office	01:00	
	4. Legal representative office	01:00	
HEI03	1. Security experts	01:25	71
	2. HR Training and development	01:00	
	3. Registrar office	01:00	
	4. Legal representative office	01:00	
HEI04	1. Security experts (x2)	02:50	00
	2. HR Training and development	01:00	
	3. Registrar office	01:00	
	4. Legal representative office	01:00	
TOTAL	***17 in-depth interviews = 19hours 30 minutes***		***385***

The profile of participants to the quantitative research is presented using SPSS in the following tables. The participation rate was 96.25% as 3.75% of questionnaires was wrongly completed others were not completed by participants at all. This means out of 400 participants who confirmed the reception of questionnaires, 385 participants completed and returned the questionnaires.

Table E.2: Participation per Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	168	43.6	43.6	43.6
	Female	217	56.4	56.4	100.0
	Total	385	100.0	100.0	

From the gender participation, all the participants correctly completed the question (total of 385 valid entries) the total number of female in general was slightly higher than that of the males. In total 217 or 56.4% of female participated to the study while 168 or 43.6% of males participated in the study. The next table presents the genders participation per institution with the Chi-Square analysis of how different is the participation presented in Table E.3.

In terms of gender participation per institution, it can be observed in the Table E.3 below that the gender participation is almost equal in the HEI02 in which the percentage of female was 41.5% while the participation of males was 41.7%, the other institutions present a slightly different levels of participation, with HEI01 a total percentage of 42.4% for females and 36.9% of females, and HEI03 has 21.4% of males and 16.1% of females participating to the research.

Table E.3: Gender * Higher Education Institution (HEI) Reference Cross tabulation

			Higher Education Institution (HEI) Reference			
			HEI01	HEI02	HEI03	Total
Gender	Male	Count	62	70	36	168
		% within Gender	36.9%	41.7%	21.4%	100.0%
	Female	Count	92	90	35	217
		% within Gender	42.4%	41.5%	16.1%	100.0%
Total		Count	154	160	71	385
		% within Gender	40.0%	41.6%	18.4%	100.0%

Table E.4: Chi-Square Tests

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.157[a]	2	.340
Likelihood Ratio	2.149	2	.341
N of Valid Cases	385		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 30.98.

The Chi-Square analysis of data shows that its value X2=2.157, df=2, and p=0.240 > 0.05. Because the p value is greater than 0.05, it can be said that there was no significant difference in the gender participation from the three HEIs.

The next profile assessment is of participants' qualifications, for this analysis, the frequencies, cross tabulation table, and the Chi-Square analysis was also presented as shown in the following three tables (Table E.5, Table E.6, and Table E.7).

Table E.5: Highest Qualification of participants

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below matric	2	.5	.5	.5
	Matric	40	10.4	10.4	10.9
	Diploma or Bachelor	87	22.6	22.6	33.5
	Honours / Postgraduate	66	17.1	17.1	50.6
	Master's	103	26.8	26.8	77.4
	Doctorate	87	22.6	22.6	100.0
	Total	385	100.0	100.0	

The association of qualifications to institutions in the Table E.5 reveals that the HEI03 has more participants with Doctorate or 44.8%, while the HEI02 had 39.1% of participants with Doctorate, and the HEI03 had 16.1% of participants with Doctorate degree. On Master's degree HEI02 has more participants than other institutions, about 53.4%, it is followed by HEI01 with 33% of participants with master's degree, while the HEI03 has 13.6% of participants with Master's degree. The order of participation with honours or postgraduate qualification is: HEI01 has 51.5%, HEI02 has 39.4% and HEI03 has 9.1%. The order of participation with diplomas of bachelors is: HEI02 has 63.2%, HEI has 32.2%, and HEI03 has 4.6%. The participation with matric qualification is HEI01 has 57.5%, HEI02 has 22.5%, and HEI03 has 20%. Lastly, the rate participation with a qualification below matric is HEI01 with 1 participant or 50% and HEI02 with 1 participant or 50%.

Table E.6: Highest Qualification * Higher Education Institution (HEI) Reference cross tabulation

			Higher Education Institution (HEI) Reference			
			HEI01	HEI02	HEI03	Total
Highest Qualification	Below matric	Count	1	1	0	2
		% within Highest Qualification	50.0%	50.0%	0.0%	100.0%
	Matric	Count	23	9	8	40
		% within Highest Qualification	57.5%	22.5%	20.0%	100.0%
	Diploma or Bachelor	Count	28	55	4	87
		% within Highest Qualification	32.2%	63.2%	4.6%	100.0%
	Honours / Postgraduate	Count	34	26	6	66
		% within Highest Qualification	51.5%	39.4%	9.1%	100.0%
	Master's	Count	34	55	14	103
		% within Highest Qualification	33.0%	53.4%	13.6%	100.0%
	Doctorate	Count	34	14	39	87
		% within Highest Qualification	39.1%	16.1%	44.8%	100.0%
Total		Count	154	160	71	385
		% within Highest Qualification	40.0%	41.6%	18.4%	100.0%

Table E.7: Chi-Square Tests

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	85.133[a]	10	.000
Likelihood Ratio	83.658	10	.000
N of Valid Cases	385		

a. 3 cells (16.7%) have expected count less than 5. The minimum expected count is .37.

The Chi-Square analysis reveals Chi-Square value X2 = 85.133, df = 10, and the p = .000 p < 0.05, because the p value is less than 0.005, it can be concluded the there was a significant difference in the qualification of the participants between the three participating HEIs. The spread of qualification had no significance on any other question that the participants were subjected to such as the attendance of ICT security training as the Chi-Square of the question “would you attend institutional IT security training related to your job level?” cross tabulated to the highest qualification of the participant is 0.034 (or p=0.043, which means p>0.05), this means there is no significant difference between the choice of attending training and the qualification of the employees.

Appendix F: Participants' quotations and views on challenges experienced that prevent them from developing end users IS security e-competencies

Participant	views or quotes
SEP01 and **SEP02** from **HEI01**	*"Lack of resources, limited budget, and shortage in human resources, and the struggle with the executives if the later do not understand the importance of the assets that you are trying to secure. Like when we are trying to implement the identity and access governance systems, some of them look at it like a software solution".*
SEP03 from **HEI02**	*"I do not have resources to ensure regular mechanism for talking to various groups in the institution and communicate different things to different people". I have got a position of IS security officer which is not filled for many occasions it was advertised. This officer could deal with ICT security in broader sense, such as liaise with various faculties and departments, he could organise workshops, and have a time to sell these activities to different levels".*
LEG2 from **HEI02**	*"The lack of IS security officer as a challenge in broader ICT security sense facing the HEI02".*
SEP03 from **HEI02**	*"The implementation of proper IS security e-competencies development programme not just a piecemeal. Like what will you do when a person is reported? Is the person going to be disciplined? You have to integrate difference role players such as change of contract to cater for high operating, the performance will be part of the process if the person is reported because of this what will be the discipline? Because people will say it is not part of the contract. It is a complex process; ensure that people take responsibility for their actions, based on that you can discipline people".*
SEP03 from **HEI02**	*"Another challenge we face is that people do not read the policy and communications which we ask them to read, then they argue that they do not know".*
REG3 from **HEI03**	*"The issue of people opening an e-mail that has got a virus attachment to it, well it is very difficult to stop that, if you have been speaking to our IT security people they tell you we try to block that e-mail before it gets to the end users but still it is getting to the end users and some people still open it, even though we tell people do not open e-mail with attachment from somebody you do not expect to get e-mail from but still it happens".*
SEP03 from **HEI02**	*"The failure of management (particularly the heads of the departments) to not get involved in the security activities such as disaster recovery management. This is part of the failure to initiate or build a security culture".*
SEP04	*"I think we can run more awareness campaign and I wish I had more*

from **HEI03**	*money to appoint the security personnel".*
SEP05 from **HEI04**	*"Non-separation of duties for system administrator who has got access to end users information is due to lack of resources as they cannot afford more people. The example, given the case of HR developer who has access to the development system but at the same time has access to data, which is not supposed to happen. This challenge is reported to the institution management as a risk as you cannot expect ICT department to do their job while they do not have resources".*
SEP05 from **HEI04**	*"Lack of monitoring across the systems, because each system has its own tools as we do not have any single tool that covers everything. Monitoring is going to be a big issue and we do not have resources for it".*
SEP05 and **SEP06** from **HEI04**	*"Not having IS security officer, which is a considerable weakness if you do not have one person who is fully responsible for that every day then you tend to manage from incident to incident".*
SEP06 from **HEI04**	*"The other regulatory framework or best practice recommendation that has impact is King iii which we are trying to comply with, again that is not an IT compliance it is an institution's compliance. It is difficult to get institution to understand especially at universities, if you talk about IT in a company you usually talk to the CIO, universities do not have to have CIOs, here you have IT which is seen as a technical function, you have got IS in teaching and learning which is over there, you have got management information in which they group a lot of CIO functions which is spread around, when you talk to the IT director you are not talking to the CIO, regulations or guidelines like King iii assumes that when you are talking to the IT you are talking to the CIO which is not, I think there is a lot of misunderstanding. I think it is a major problem for universities and it is getting worse and worse because we now need to comply with these legislations. This challenge relates to lack of management commitment to coordinate IT systematically, the IS security and IS security e-competencies development".*

Appendix G: Participants' quotations and views on IS security threats faced in their respective HEIs

Participant	views or quotes
SEP01 and **SEP02** from **HEI01**	*"among the threat mentioned include: internal people make sensitive research information that is not supposed to be made public that is typically one thing there are a lot of that and to have control of all of that it is quite difficult, internal user level distraction and down time in productivity due to viruses and malware attacks, there could be embarrassment when ICT system down time, possibility of hacking into social media account that can expose the institution, abuse of IS resources which did not happen 20 or 30 year ago, people not taking responsibility for their IS resources that can lead to complacency and allowing viruses to attack the network, fear of exam paper being compromised because they are on the network (which is a big threat), having end users who might not identify that this is a security threat. We had at the HEI01 had been affected by the denial of hard drive access attack which didn't come necessarily through the firewall because it could be from USB from home. So it is the internal users that are the biggest threat".*
REG1 from **HEI01**	*"If* student are selected and the system sends an acceptance letter to all the students who were declined that is fatal*".*
SEP03 from **HEI02**	*"The lack of resources to handle the threats is a threat because there is a responsibility for ICT to play a role in making sure that security is properly communicated and security policy is implemented, we do not have resources for that, not reading communications and policies are a threat as people can claim that they do not know. One incident we have suffered is that of the person stole someone else account and transferred money into his own account, but we got it back it was not a loss, but it did happen".*
LEG2 from **HEI02**	*"Threat linked to tender procedures in which the internal person might disclose information related to the tender".*
SEP05 from **HEI04**	*"Disgruntled employees are high security threat; altering information like students marks. Having old systems that deal with information and the changes in legislation such as credit Act and the institution does not comply can expose the institution to huge risks if this is not corrected quickly. Likewise, students can take the university to court for non-execution of the policy, having end users who cannot know and identify the threat (good example is phishing attempts and spam attempts I can see even senior people with a fairly good technical background who cannot distinguish what is genuine threat and what is not".*
SEP06	*"Sending or forwarding of confidential information through e-mail is threat. In HR division where somebody loaded up something into the*

from **HEI04**	*wrong place and breached the confidentiality on our recruitment system".*
SEP06 from **HEI04**	*"Research from the HEI04 that became a policy in government and now there are question marks about that policy and now you need to go back to the research data, it is not there anymore. That is a serious risk for the university as well, the stuff on which the policy is based is no longer there anymore because the data is gone with the researcher when he left the university".*
SEP01 and **SEP02** from **HEI01**	*"There are a lot of scandals about fake degrees and that can put the institution under reputation damage, so we must prevent against that, raise more awareness of those types of threats. The participants mentioned also the fear of exam paper being compromised because they are on the network".*
SEP04 from **HEI03**	*"The issue of a degree to undeserving student as one of the threats that you cannot be forgiven".*
REG3 from **HEI03**	*"Insurance of strict integrity is the most critical because the integrity of our students' records is crucial to our reputation. If students go out and say they come from this institution and our official records do not have such a student it is a damage to our reputation then we are finished as nobody can believe in this institution".*
SEP05 and from **HEI04**	*"The most damaging one would be the one that damage the reputation of university. In terms of reputation the most damaging ones are those that are not IS security related, there was an incident where the financial controls were inadequate and there was fraud and when the audit of that was done beside the lack of financial controls there was also technical issues in getting back to the information as this incident stretch back as far up to 10 years and it was impossible to get some of the old information because of technical reasons".*

Appendix H: Expert views and quotations on the object of IS security e-competencies development

Expert	Experts views and/or quotes
EXP12	*Information security is not just like a domain of information security specialists, everyone needs to know about information security.*
EXP13	*The security of IS resources I am using is both my responsibility and the institution, my responsibility because I have to make sure that I do not go and surf on the dangerous websites and I protect my password so that no one can access the resources when I am not around. But it is the institution's responsibility because it has to put in place technologies that prevent people from hacking into my system.*
EXP07	*I would certainly not only attend the training but I will love also to be involved in the training.*
EXP09	*I will support training that is one of the important aspects of information security. If I am very good in Information security and then I have another employee that does not know anything about information security through that person I might have problems with the whole organisation.*
EXP09	*What is necessary is for anybody who is using computer or any device that is related to data or information you need to provide certain kind of knowledge of how to protect the computer, the data and information.*
EXP10	*Yes, the training of end users on IS resources security is very important and I will absolutely support the IS security training.*
EXP12	*Yes of course I will be able to attend and support it, and if I have employees under my leadership I will allow them to attend as well.*
EXP13	*I will support the IS security training and awareness, and it is very important and I will definitely allow employees under my control to attend it.*
EXP15	*I will support the IS security training and everyone needs IS security training and skills.*

Appendix I: Participants' views on the importance of ICT resources in the HEI environment

Participant	Views and/or quotes
SEP01 **from** HEI01	*"If you are at the leading edge of researches that can have commercial benefits for the university and the nation, then you have to safeguard them, I think those are the things we are becoming more aware of than in the past".*
REG1 **from** HEI01	*"ICT resources are core to business of HEI because the entire student administration, from application to registration, examination, uploading of marks, finances, residences, the management of contact centre, and academic programme management, all are managed on ICT platform. So if anything (forcefully or error that can affect the systems) happens to ICT platform, the registrar cannot register, which cause problems in the entire flow of information to other departments".*
REG2 **from** HEI02	*"The discussion on the importance of ICT resources has been discussed at the council level. There is an understanding at the institution that ICT resources are important for the institution, because now more than anything, ICT is the anchor to the university and our vision and strategic objectives are supposed to be driven through ICT and it is our platform and it is recognised as such by the council".*
REG3 **from** HEI03	*"ICT and the whole system of examination and graduation is mechanised and it could not be completed without the support of ICT resources which are also vital in the support of teaching and learning and research. ICT is not our core business, but it is core to our business as there is no course at this institution that does not rely on ICT, and there is virtually no research that does not involve some form of ICT support whether it is simply the web or more than that, and the administration is totally dependent upon functioning ICT".*
REG4 **from** HEI04	*ICT as very important component of university structure, 30 years ago there was no ICT systems like computers, you send telegrams, and you send letters. Nowadays you see e-mails, we correspond with our students who apply at the institution through ICT, and we publish and send marks through ICT, so now ICT is absolutely integral part of HEI.*

Appendix J: Participants' views on the critical ICT systems in their institutions

Participant	Views and/or quotes
SEP01 **from** HEI01	*"In no particular order the critical systems include HR system, student administration system, the financial system, the leaning management system, and the e-mail system as well".*
SEP03 **from** HEI02	*"The focus is on their ERP system because that is where their finances and students' records are. The participant mentioned also the network infrastructures, the blackboard or e-learning system, the exchange system for e-mail, the personal computers in the labs and Microsoft systems that deal with all elements such as research, academic and administration type of environment".*
SEP04 **from** HEI03	*"The network system which if it goes down, everything else goes down, financial system, the procurement systems, the learning management system, and the system that manage the awarding of qualifications as also critical. Due to their processing of human and health sciences and military projects, these research systems are also critical to the institution".*
SEP06 **from** HEI04	*"The finance system is critical because creditors and debtors cannot be dealt with, HR system because if it is down people cannot be paid, students information is extremely important, the order management system (procurement) is important as all orders are done electronically, there will be a lot of problems if teaching and learning management system is down, research management system is important as the research income which is about 2 billion of rand per annum and need to be reported to the government in order to get subsidy income will be affected if the system is not working, and the people who are custodians of the information from these systems are also critical".*
SEP01 **from** HEI01	*"To undertake actions such as encryption you need to have some sort of data classification for any organisation. You have to understand from business what is sensitive and what is not sensitive, and we have not driven this and I think it is not IT job to do it, we will implement the controls for encryption but the business must tell us, and I do not think that they got that is their mind".*
SEP03 **from** HEI02	*"We have done some sort of classification based on data managers themselves, but it does not mean that we have done much detail than that".*

Appendix K: Participants' views on the IS security e-competencies development in their institutions

Participant	Views and/or quotes
SEP01 **and** SEP02	*The institution has in the distant past made it part of induction programme and had a voluntary security awareness coupled to e-mail training. The practice fallen away because it was not compulsory and the institution falls short on policy training and awareness as no training has ever been provided on ICT security policy.*
SEP02 **from** HEI02	*The institution has not provided IS security training to the end users. They have done some exposure to different aspects during the induction or provided some information on their website, but the coherent training exercise should be done.*
SEP04 **from** HEI03	*The institution does not run security training per says, but some aspects are incorporated in the normal training as SAP like do not share the password or leave it somewhere. During the security campaign, antivirus and identity information is provided on the website.*
SEP05 **from** HEI04	*ICT security awareness and training are critical, but these are the things they the institution has neglected the big problem we have with the current induction programme is there is no slot for IT exposure.*
SEP06 **from** HEI04	*The institution has not done any formal training on ICT security. The assumption can be made that the senior people in the institution such as the registrar know very well about ICT security even if they never had been trained. The ICT security policy does not prescribe for the training of end users on IS security.*

Appendix L: Participants' views on the identification and categorisation of critical IS resources end users in their institutions

Participant	Views and/or quotes
SEP01 **and** SEP02 **from** HEI01	*"Everyone who is using ICT resources is a key end user, starting from students, research staff, support staff, and academic staff. Besides these users, there are also NGOs and contractors that are allowed on the campus".*
SEP03 **from** HEI02	*"Categorised the end users in students, the staff, and the super users who are part of the staff who deal with the application of policies, and the system administrators. We have data managers who do not need to have access, but authorise access and they need also training".*
SEP04**from** HEI03	*"Most critical end users are the system administrators because they have got access to almost everything, and then the developers. We have three types of end users in our portfolio are divided: the first group is made of administration, then teaching and learning users, and the end users in research department".*
SEP05 **from** HEI04	*"We rely heavily on the concept of information curator, their responsibility and accountability. The information curator or his or her delegated people must set the roles and access right and operating procedures. That is very important part and if not done properly, it will be a big risk, and it is something which in the past people viewed it as an IT responsibility, but in reality it is not IT responsibility but the curator. If it is financial information it is the chief financial director who is a curator, if it is peoples' information it is the chief director of human resources, and if it is students' information and marks it is the registrar who is the curator. On the next level we have got the information managers who are typicality super users, people that are responsible for implementing the policy within the end user department, and bellow them there is a next group of users who have more right than average employees because of their position are the financial officers who can sign on large amount of money, and procurement officer etc.".*
SEP06 **from** HEI04	*"In the end user department we have a curator of information), for instance in HR division the head of HR he understands that he is responsible for the security of the HR data, so those things we have identified and what their responsibilities involve, in other words it is not the IT that is responsible for their data, its them that are responsible for their data, IT gives them the tools to manage the data".*

Appendix M: Participants' views on the training challenges in general

Participant	Views and/or quotes
TRD1 **from** HEI01	*"Most of the training sessions are offered on the main campus, there is a need to identify other means of delivering training such as online. There are also challenges related to limited budget, the scheduling of training to accommodate conflicting schedules of academics and administration and support staff, and cancellation of training by the staff members after the registration".*
TRD2 **from** HEI02	*"People want to come to training and they want to engage but they have too much work. Other challenges like people attitude, they come to training but they have got the attitude of what is the point of coming here but they do not see how it can make a difference in their lives. The other challenge is related to staff complement, and the dispersion of training budget to individual department which the central training and development cannot control if it is used for the training as required".*
TRD3 **from** HEI03	*"Organising training when you have got so many campuses it is a challenge in that most of the earning take place at main campus. However, when the staffs need the training they have to travel. The other challenges mentioned are related to a limited budget for training as there has been budget cut for the last three years. Another challenge would be management of the relevancy of the skills, the continuous work round matching the right programme to the right skill, and then getting the right group of people in the classroom".*
TRD4 **from** HEI04	*"Lack of IT security officer who is also important in the coordination of the IS security training programmes and a limited budget as the biggest challenges. Besides, each functional area and unit organises its own trainings according to their needs".*

Appendix N: Participants' views on the approaches to training

Participant	Views and/or quotes
SEP05 **from** HEI04	*"Risk of viruses where we do not have the opportunity to train them but through newsletters and information sessions we try to make every user on campus aware of risks".*
SEP04 **and** REG3 **from** HEI03	*"We run awareness campaigns like simple things like do not open e-mail if it has got .exe file in it, we say it over and over in our e-mails that go from the help desk saying we will never ask you your user name and password, never we do that and run campaigns that banks are running. The running of this kind of campaign needs to support the training session as many people do not read communications or do not understand the implications for ICT security threats".*
SEP05 **from** HEI04	*"The awareness is provided through newsletters and publications; the second is through regular information sessions with the IT staff, if it is the rest of the university it must be through newsletters and electronic publications and emails if there is immediate security threat. Again it is difficult to assess if employees read the newsletters".*
TRD3 **from** HEI03	*"Training is open to all staff members (permanent and on contract), and induction programme is used to introduce the newly appointed staff members to the operation of their institution".*
TRD2 **from** HEI03	*"The current practice on the identification of training need is through line managers' suggestion, conduction of surveys, information gathering in way staff meeting with line managers, or schedule training as they align to the achievement of institution's objective".*
TRD1, TRD2, TRD3, **and** TRD4	*"The participation to all training sessions is not compulsory. The only advantage employees get is to get skills and an opportunity to compete for promotional position when they become available".*