

**A FRAMEWORK TO INTEGRATE INFORMATION AND  
COMMUNICATION TECHNOLOGY SECURITY  
AWARENESS INTO THE SOUTH AFRICAN EDUCATION  
SYSTEM**

**by**

**MVELO WALAZA**

**submitted in accordance with the requirements**

**for the degree of**

**MASTERS IN COMPUTING**

**at the**

**UNIVERSITY OF SOUTH AFRICA**

**SUPERVISOR: PROF. M. LOOCK**

**CO-SUPERVISOR: PROF. E. KRITZINGER**

**2017**

## Executive Summary

Many countries use Information and Communication Technology (ICT) to improve and enhance the levels and standards of their education systems. A number of scholars in South Africa have conducted studies with the aim of proving that ICT can play a major role in improving the quality of education in the country. This study investigates the problem of the lack of ICT security awareness in South African education (among the South African school learners). The literature review that has been conducted has shown that there is a huge problem when it comes to integrating ICT security awareness into the South African schooling system.

This research aims to propose a framework to the relevant authorities and interested parties that will assist with the integration of ICT security awareness into the South African schooling system.

## Keywords

ICT; ICT Security; education; models; frameworks; security; awareness; school learners

# Table of Contents

Table of Figures.....	viii
Abstract.....	xi
Declaration.....	xiii
Acknowledgements.....	xiv
Dedication.....	xiv
Chapter 1: Introduction .....	1
1.1    Introduction .....	2
1.2    Research Problem .....	4
1.2.1    Problem Statement.....	4
1.2.2    Research Questions.....	5
1.2.3    Research Objectives .....	6
1.2.4    Research Methodology .....	7
1.2.5    Structure of the Dissertation .....	8
1.3    Limitations and Scope of the Study .....	10
1.4    Summary .....	10
Chapter 2: ICT in Education.....	11
2.1    Introduction .....	12
2.2    ICT in Education .....	12
2.3    ICT in Education in Other Countries.....	13
2.4    ICT Usage in South African Education.....	14
2.5    Advantages and Disadvantages of Using ICT in Education .....	16
2.5.1    Benefits of Using ICT in Education .....	16
2.5.2    Disadvantages and Limitations of Using ICT in Education .....	18
2.6    Challenges of Integrating ICT in Education .....	19
2.7    Potential ICT Security Threats Facing School Learners .....	20
2.7.1    Social Media .....	20
2.7.2    Cyber-Crime .....	21
2.7.3    Instant Messaging .....	22
2.7.4    Sexting and Exposure to Sexual Activities.....	22
2.7.5    Social Engineering .....	22
2.7.6    Cyber-Bullying .....	22
2.7.7    The 419 Scams .....	22
2.7.8    Bluesnarfing .....	23

---

2.9	Conclusion.....	23
Chapter 3: ICT Security.....		24
3.1	Introduction .....	25
3.2	ICT Security in the World .....	26
3.2.1	The Three Primary Concepts of Information Security .....	27
	Availability.....	27
	Confidentiality.....	27
	Integrity.....	28
3.2.2	ICT Security Standards .....	28
	ISO Standards.....	28
	Payment Card Industry Data Security Standard .....	29
	COBIT.....	29
	ITIL (OR ISO/IEC 20000 Series) .....	29
3.3	The Need for ICT Security .....	29
3.4	ICT Security Threats .....	30
3.4.1	Virus Threats .....	31
3.4.2	Spyware Threats.....	31
3.4.3	Hackers.....	31
3.4.4	Trojan Horse.....	31
3.4.5	Phishing Threats.....	32
3.4.6	Pharming Threats.....	32
3.4.7	Adware and Advertising Trojans .....	32
3.4.8	Unsecured Wireless Access Points.....	32
3.4.9	Social Engineering .....	32
3.5	Countermeasures Against ICT Security Threats.....	33
3.5.1	Prevention.....	33
3.5.2	Detection.....	33
3.5.3	Reaction .....	34
3.5.4	Identification and Authentication.....	34
3.5.5	Authorisation and Access Control.....	34
3.5.6	Information Security Awareness.....	35
3.6	ICT Security Awareness .....	35
3.6.1	The Need for Effective ICT Security Awareness among School Learners .....	36
3.7	ICT in South Africa.....	37
3.7.1	ICT Security Awareness in South Africa .....	39

---

3.7.2	ICT Security Awareness in South African Education .....	42
3.8	Conclusion.....	43
Chapter 4: Models and Frameworks.....		44
4.1	Introduction .....	45
4.2	ICT Security Awareness Models and Frameworks.....	46
4.2.1	The Business Model for Information Security .....	47
4.2.2	The Information Security Retrieval and Awareness Model .....	48
4.2.3	The Comprehensive Information Security Framework.....	49
4.3	ICT-in-Education Models and Frameworks.....	50
4.3.1	The Four in Balance Model .....	51
4.3.2	The Teacher Development Framework .....	52
4.3.3	Model for ICT Rural Education .....	54
4.4	Conclusion.....	55
Chapter 5: Research Methodology .....		56
5.1	Introduction .....	57
5.2	Research Design.....	57
5.2.1	Research Philosophy – Interpretivism .....	58
5.2.2	Research Approach – Inductive Approach.....	59
5.2.3	Methodological Choice – Multimethod Qualitative Study .....	61
5.2.4	Research Strategy – Phenomenology .....	61
5.2.5	Techniques and Procedures.....	62
	Data Collection Techniques .....	62
	Literature review.....	62
	Online Questionnaires (Focus Group 1).....	62
	Peer-reviewed Academic Conferences (Focus Group 2) .....	64
	Data Analysis – Inductive Analysis .....	65
5.2.6	Verification – Proof of Concept.....	66
5.3	Conclusion.....	67
Chapter 6: The Design of the SAISAFE .....		68
6.1	Introduction .....	69
6.2	Analysis of Models and Frameworks .....	70
6.3	The Analysis of Models and Frameworks Results.....	72
6.4	Conclusion.....	73
Chapter 7: Discussion of the building blocks .....		74
7.1	Introduction .....	75

---

7.2	The Building Blocks – Overview .....	75
7.2.1	Leadership and Governance .....	75
7.2.2	User Awareness .....	76
7.2.3	Information Security Documentation .....	78
7.2.4	Policies and Standards .....	79
7.2.5	Code of Best Practice .....	79
7.2.6	Human Factors .....	80
7.2.7	Collaboration and Support.....	80
7.2.8	ICT Learning and Training Centres .....	81
7.2.9	Measuring and Monitoring .....	82
7.2.10	Innovation and Technology.....	83
7.2.11	Incident Management.....	83
7.2.12	Compliance.....	84
7.2.13	School Learners.....	85
7.3	An Overview of the Added Components .....	86
7.3.1	Language .....	86
7.3.2	ICT Security Ombudsman.....	87
7.3.3	ICT Security Curriculum.....	88
7.3.4	Information Repositories .....	89
7.3.5	Summary of the Added Components.....	90
7.4	The South African ICT Security Awareness Framework for Education (SAISAFE).....	90
7.4.1	Leadership and Governance .....	91
7.4.2	User Awareness .....	91
7.4.3	Documentation .....	92
7.4.4	Collaboration and Support.....	93
7.4.5	People .....	94
7.5	Conclusion.....	97
Chapter 8: Analysis and Findings .....		98
8.1	Introduction .....	99
8.2	Summary of the questions.....	101
8.2.1	The problem with the integration of ICT into the South African education system... 102	
8.2.2	The advantages and disadvantages of the SAISAFE.....	102
8.2.3	The readability of the SAISAFE .....	104
8.2.4	The viability of the SAISAFE.....	104
8.2.5	Contribution of the SAISAFE to the quality of education in South Africa.....	104

---

8.2.6	Contribution of the SAISAFE towards integrating ICT security awareness into South African education.....	105
8.2.7	Meaningful contribution to the overall South African education system .....	105
8.2.8	Relevance of building blocks to South Africa.....	105
8.2.9	Meaningful contribution of the SAISAFE to ICT Security Awareness in education.....	106
8.2.10	Usage of the SAISAFE for future research.....	106
8.2.11	Implementation of the SAISAFE .....	106
8.2.12	Overall rating of the SAISAFE .....	107
8.2.13	Contribution made by formulating the proposed framework.....	107
8.3	Conclusion.....	107
Chapter 9: Conclusions and Future Research .....		108
9.1	Introduction .....	109
9.2	Conclusions .....	109
9.3	Future Research .....	110
9.4	Re-visiting the Research Questions .....	110
9.5	Contributions of this research .....	113
9.5.1	Academic Contribution .....	113
9.5.2	Practitioner Contribution .....	114
9.6	Conclusion.....	115
References .....		116
Appendices.....		129
Appendix A: Accepted Research Article – SAICSIT2014.....		130
Appendix B: Accepted Research Article – ISTE2015 .....		162
Appendix C: Accepted Research Article – InfoSec2015 .....		187
Appendix D: Questionnaire.....		211

## Table of Figures

Figure 1.1: The Diagrammatic Representation of the Research.....	9
Figure 2.1: The CIA Triad (Andress 2011) .....	<b>Error! Bookmark not defined.</b>
Figure 4.1: The Business Model for Information Security (ISACA 2009) .....	47
Figure 4.2: The ISRA Model (Kritzinger 2006).....	49
Figure 4.3: The Comprehensive Information Security Framework (Da Veiga 2008).....	50
Figure 4.4: The Four In Balance Model (Draper 2010) .....	52
Figure 4.5: The Teacher Development Framework (Department of Education 2007).....	53
Figure 4.6: Model for ICT Rural Education (Roy 2012) .....	54
Figure 5.1: Research Outline (based on Swanepoel 2015).....	58
Figure 5.2: Inductive analysis process (adopted from Swanepoel 2015).....	60
Figure 6.1: The Analysis of Models and Frameworks Results.....	73
Figure 7.1: The Added Components.....	90
Figure 7.2: The Documentation Component.....	91
Figure 7.3: The Collaboration and Support Component.....	92
Figure 7.4: The People Component.....	94
Figure 7.5: South African ICT Security Awareness Framework for Education (SAISAFE).....	96
Figure 9.1: The SAISAFE.....	113

## List of Tables

<b>Table 6.1: The Analysis of Models and Frameworks</b> .....	71
---	----

## Definition of Terms

ATM	Automated Teller Machine
Awareness	The ability to perceive, to feel or to be conscious of events, objects, thoughts, emotions, or sensory patterns (Wikipedia)
BMIS	Business Model for Information Security
Building blocks	Components that have been derived from the various models and frameworks that exist in literature
CIA triad	Confidentiality Integrity Availability triad
CISF	Comprehensive Information Security Framework
COBIT	Control Objectives for Information and related Technology
DoC	Department of Communications
DBE	Department of Basic Education
DHET	Department of Higher Education and Training
DTPS	Department of Telecommunications & Postal Services
ECT Act	Electronic Communications and Transactions Act
ENISA	The European Network and Information Security Agency
E-Safety	The knowledge of maximising the user's personal safety and minimising security risks to private information and property associated with using the internet, and the self-protection from computer crime in general (Wikipedia)
HKSAR	Hong Kong Special Administrative Region
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IM	Instant Messaging
ISACA	Information Systems Audit and Control Association
SAISAFE	South African ICT Security Awareness Framework for Education

ISG Africa	Information Security Group of Africa
ISP	Internet Service Providers
ISRA	Information Security Retrieval and Awareness
ISSA	Information Security South Africa
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
MITM	Man-in-the-Middle
NMMU	Nelson Mandela Metropolitan University
PAIA	Promotion of Access to Information Act
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
SABRIC	South African Banking Risk Information Centre
SITA	State Information Technology Agency
UFH	University of Fort Hare
URL	Uniform Resource Locator

## Abstract

There is general consensus about the importance of Information and Communication Technology (ICT) security in South Africa. This consensus is evident from initiatives related to the formulation of legislation and policies like the Electronic Communications and Transactions (ECT) Act and the National Cyber Security Policy. A number of South African academic institutions have also come on board with initiatives aimed at enhancing ICT security awareness all over the country. In fact, ICT security awareness has been classified as an important component of South Africa's national security.

Many countries use ICT to improve and enhance the standard of their education systems. A number of scholars in South Africa have conducted studies with the aim of proving that ICT can play a major role in improving the quality of education in the country. The research in hand investigates the lack of integration of ICT security awareness into the South African education system. The literature review that was conducted reveals that there is a huge problem especially when it comes to the integration of ICT security awareness into the South African schooling system.

The advancement of technology has come with a number of advantages and disadvantages. The easy access to information via the internet, coupled by unsupervised access to instant messaging applications (Skype, MXIT) and social media platforms (Facebook, Twitter and many more), hugely increases the vulnerability of school learners to ICT security attacks and ICT-related crime. The current research therefore investigates the vulnerability caused by the lack of ICT security awareness among school learners as one of the main disadvantages of the advancement of information technology.

An analysis of existing models and frameworks in the two spheres of ICT, namely education and ICT security was conducted. The aim was to determine any similarities or overlap between these spheres and to determine whether the existing ICT models and frameworks are relevant to South Africa. The analysis showed a significant disparity and inconsistency between the two spheres and proved that there is a definite need for a framework (relevant to South Africa) that can be used for the integration of ICT security awareness into South African education. Hence, the researcher proposed a more integrated approach in the form

of a framework that is directed at South African school learners, based on an in-depth literature review of past scholarly work, models and frameworks. Having reviewed a number of existing models and frameworks, and identifying the potential gaps, the researcher proposed a framework to address the lack of integration of ICT security awareness into the South African education system. The proposed framework, called the South African ICT Security Awareness Framework for Education (SAISAFE), was reviewed for its potential applicability in the South African context, and the results of the literature review analysis are reported to support the analysis of models and frameworks.

# Declaration

Student Number: 53315804

I declare that **A FRAMEWORK TO INTEGRATE ICT SECURITY AWARENESS INTO THE SOUTH AFRICAN EDUCATION** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

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

---

SIGNATURE

MR MVELO WALAZA

---

DATE

## Acknowledgements

*“For I know the plans I have for you, declares the Lord, plans to prosper you and not to harm you, plans to give you hope and a future”  
- Jeremiah 29:11-*

I would like to thank my Lord and saviour for the guidance, strength and the resilience to continue with this dissertation. Without Him, I would not have been able to achieve this.

My sincerest gratitude goes to the following people:

My supervisors, Professor Marianne Loock and Professor Elmarie Kritzinger for their continued support, patience and encouragement;

My wife (Somikazi) and daughter (Qhayiya) as well as my three sisters (Phumla, Akhona and Zimbini) for prayers, encouragement, love and their belief in me throughout this process;

My critical reader, Dr. Johan van Loggerenberg for his commitment and dedication in editing my dissertation and providing constructive criticism that assisted me to complete this work.

## Dedication

To my late father (Velile Godfrey Walaza) and brother (Masande ‘Prince’ Walaza) – Rest In Peace.

To my mother (Zithelile Elizabeth Walaza), you are my inspiration.

# Chapter 1: Introduction

## 1.1 Introduction

Information Communication Technology (ICT) is used in many countries across the world (Amedzo, 2007). A number of software applications such as Facebook, Twitter and WhatsApp have been developed to facilitate communication between users from different locations all over the world (Nevondwe and Odeku, 2014). Companies make use of technologies such as Skype to communicate in real time with their counterparts located far away from one another in different geographic places. Developing countries such as South Africa have eagerly adopted this trend of using ICT for communication, and are utilising the advantages that it offers wherever possible.

South Africa uses ICT in all spheres of industry – in academia, in business, in sports, in government departments – to name but a few. The increasing usage of ICT in South Africa has obviously triggered wide concern about ICT security awareness. In recent years, a growing number of ICT-related crimes have been reported in South Africa (Belayneh, no date), ranging from cyber-attacks to online banking fraud conducted at one of the largest banking institutions in the country. Since the future corporate sector and government departments will be run by the learners who are currently at school, it is essential that they be equipped with the necessary ICT security skills. The focus of the current research is therefore on school children, and aims to alert them to the dangers of ICT and equip them to deal with information security concerns in an attempt to curb the ICT-related crime in the country.

Studies have confirmed that there is a significant increase in the usage of ICT by school learners in South Africa (MyBroadband 2014; Kreutzer 2009). Hence, there is a definite need for introducing ICT security measures and ICT security awareness initiatives in order to protect these learners. The usage of ICT by school learners has a number of benefits and advantages – these include access to information, access to the internet, and learning new skills. Tertiary institutions such as the University of South Africa (UNISA) make use of ICT to communicate with their students who are scattered all over the world. School learners make use of ICT resources such as mobile phones, emails, instant messaging, and social networks to communicate and collaborate with their peers. Studies have also shown that ICT has improved teaching and learning in schools where it is used (Higgins, 2003).

Despite the benefits associated with school learners' usage of ICT, it also has numerous disadvantages. ICT usage exposes school learners to various ICT-related risks and threats in the form of virus attacks, spyware, social engineering, phishing, and pharming. Other risks related to ICT usage among school learners is exposure to child pornography and human trafficking. It is therefore imperative that school learners are made aware of ICT security at a young age so that they grow up knowing the real dangers associated with ICT usage. The importance of enhancing ICT security awareness among school learners from a young age has been confirmed by the suggestions by reputable scholars to include ICT security awareness in the school curriculum (Kritzinger & Padayachee 2007; Walaza, Looock & Kritzinger 2014). This research proposes an ICT security awareness framework constructed on the basis of various existing frameworks and models.

ICT security awareness and the protection of individuals constitute a major challenge for security experts, scholars, and politicians (Dlamini and Modise, 2012). In their research, Dlamini and Modise (2012) identified a number of ICT security awareness initiatives launched by local academic institutions such as the Nelson Mandela Metropolitan University (NMMU), University of Fort Hare (UFH) and University of South Africa (UNISA), as well as private institutions such as the South African Banking Risk Information Centre (SABRIC) and Information Security Group of Africa (ISG Africa). However, the literature review that they conducted shows that there is still a need for greater intervention when it comes to ICT security awareness in South Africa.

The available literature in this field contains a number of models and frameworks related to ICT security awareness as well as ICT in education. The first of the ICT security awareness models and frameworks is the Business Model for Information Security, a model that uses the business approach to ICT security. According to ISACA (the Information Systems Audit and Control Association) (2009), a strong point of this model is that can be adapted for different kinds of environments. The Information Security Retrieval and Awareness model, which focuses on the ICT security awareness angle, can according to Kritzinger (2006) be used to enhance information security awareness of employees in an organisation. The Comprehensive Information Security Framework (CISF) is a framework that can be used in different types of environments (Da Veiga, 2008). The Four In Balance model is the first of the ICT-in-education models and Draper (2010) claims that this model adds value to the

teaching and learning methods. The Teacher Development Framework that was proposed by the South African Department of Education in 2007 serves as a guide for educators to assess their levels of ICT skills and knowledge. The Model for ICT Rural Education is a model that was developed for the integration of ICT into rural education in India (Roy, 2012). All of these models and frameworks will be discussed in more detail in the paragraphs that follow.

A shortcoming that was identified when the models and frameworks were analysed, was that the existing frameworks and models do not include ICT security awareness in education and they are not necessarily relevant to the South African context. For instance, the issue of home language is not addressed in any of the models or frameworks. Thus, the South African ICT Security Awareness Framework for Education (SAISAFE) proposed in this research attempts to address this shortcoming by including components that will assist with the integration of ICT security awareness in South African education. The purpose of the proposed framework is to bridge the gap between the ICT security awareness models and frameworks and the ICT-in-education models and frameworks, and to present a framework that is relevant to South Africa.

## 1.2 Research Problem

This section discusses the problem statement, research questions, objectives, deliverables, as well as the research methodology used. A diagrammatic representation of the research is also given in this section. To enable the formulation and proposal of a suitable solution for the problem identified in this research, a problem statement was formulated.

### 1.2.1 Problem Statement

According to Kreutzer (2009), ICT is to an increasing extent used by South African school learners. This increasing usage causes concern, because many school learners do not have the necessary knowledge to protect themselves against the dangers associated with ICT usage. Literature reveals that there has not been sufficient integration of ICT security awareness into the South African education system. Scholars such as Kritzinger (2006) have argued for the inclusion of ICT security awareness in the South African school curriculum, to no avail (De Lange and Von Solms, 2013). The inclusion of ICT security awareness in the

school curriculum should benefit and increase awareness among South African school learners (Kritzinger and Padayachee, 2007).

The curriculum issue is further observed by Wayman and Kyobe (2012) who caution that South African academic institutions have not integrated the social aspects of ICT security awareness into their curricula. Their literature review revealed a gap between ICT security awareness and ICT in education in South Africa. It also revealed that no framework exists that can be used for the integration of these two spheres. The problem addressed in this research is therefore summarised as follows:

*Because ICT security awareness is not adequately addressed in the South African school curriculum, school learners are unaware of the dangers involved in ICT usage, thereby exposing themselves to personal and societal risk.*

ICT security awareness is an important aspect of the education of school learners. Insufficient ICT security awareness can expose the vulnerabilities of technology users (Kritzinger & Von Solms 2010). It is of vital importance that ICT security awareness is taught to school learners at a young age so that they are aware of the dangers posed by ICT from an early age (Kritzinger and Padayachee, 2007). One way to do this is by integrating ICT security awareness into the South African education system.

### 1.2.2 Research Questions

As a result of the lack of ICT security awareness in the South African education system, Kritzinger and Padayachee (2007) state that it is important for school learners to be introduced to and taught about information security at an early stage in their lives. The following research questions aim to ensure that this can be accomplished.

- Can the existing models and frameworks be used for the integration of ICT security awareness into the South African education system?
- Is there a gap between the ICT-in-education models and frameworks, and the ICT security awareness models and frameworks?

- Which building blocks derived from existing models and frameworks can be used to formulate and propose a framework that can be used for the integration of ICT security awareness into the South African education system?
- What framework can be used to integrate ICT security awareness into the South African education system?

These research questions were formulated to address the problem statement. The objectives of this research will be discussed next.

### 1.2.3 Research Objectives

In response to the research questions in the previous section, the following objectives were formulated:

- To conduct a literature review to determine whether the existing models and frameworks can be used for the integration of ICT into the South African education system.
- To conduct a gap analysis between the two spheres of ICT-in-education models and frameworks, and ICT security awareness models and frameworks.
- To determine the building blocks derived from existing models and frameworks that can be used to formulate a framework for the integration of ICT security awareness into the South African education system.
- To propose a framework that can be used to integrate ICT security awareness into the South African education system.

The aim of these research objectives is to assist in proposing a workable framework that can be used for the integration of ICT security awareness into the South African education system. The research methodology employed in this research is introduced in the next section, and a more detailed discussion follows in Chapter 5.

### 1.2.4 Research Methodology

The qualitative research method was chosen as the research methodology used in this research. According to Hancock, Ockleford and Windridge (2009), qualitative research attempts to broaden our understanding of how things came to be the way they are in the world. The current research investigated ICT security awareness in South African education and subsequently proposed a framework that can be used to integrate ICT security awareness into the local education system. Hancock et al. (2009) state that the qualitative research method is also used when one has to assess whether a new service is implementable. It is for these reasons, among others, that the qualitative research method was chosen for the current research.

The researcher used an in-depth literature review and made an analysis of models and frameworks to determine the extent of ICT security awareness in education. The information gathered from the literature review and the analysis of models and frameworks conducted was subsequently used as building blocks to construct and formulate a framework for this research.

Another reason and motivation for the selection of the qualitative research method was the fact that it permits the usage of flexible data collection techniques and tools such as academic literature reviews, questionnaires and structured interviews with research participants (Hancock, Ockleford and Windridge, 2009). This methodology enables one to gain insight into the mind and reasoning of research participants by using questionnaires. Academic and industry experts were asked to provide their insights and their views on the suitability and practicality of the proposed framework.

The identified experts (and their companies) who were used during the initial evaluation of this framework were from the Gauteng province of South Africa. By using a questionnaire as the qualitative research method, the researcher was able to make an effective qualitative determination of the behaviour, thoughts and opinions of the academic and industry experts in ICT security. As is the norm during qualitative research, a framework based on the findings of the research was proposed as a solution to the research problem. In the next section, the structure of the dissertation is discussed.

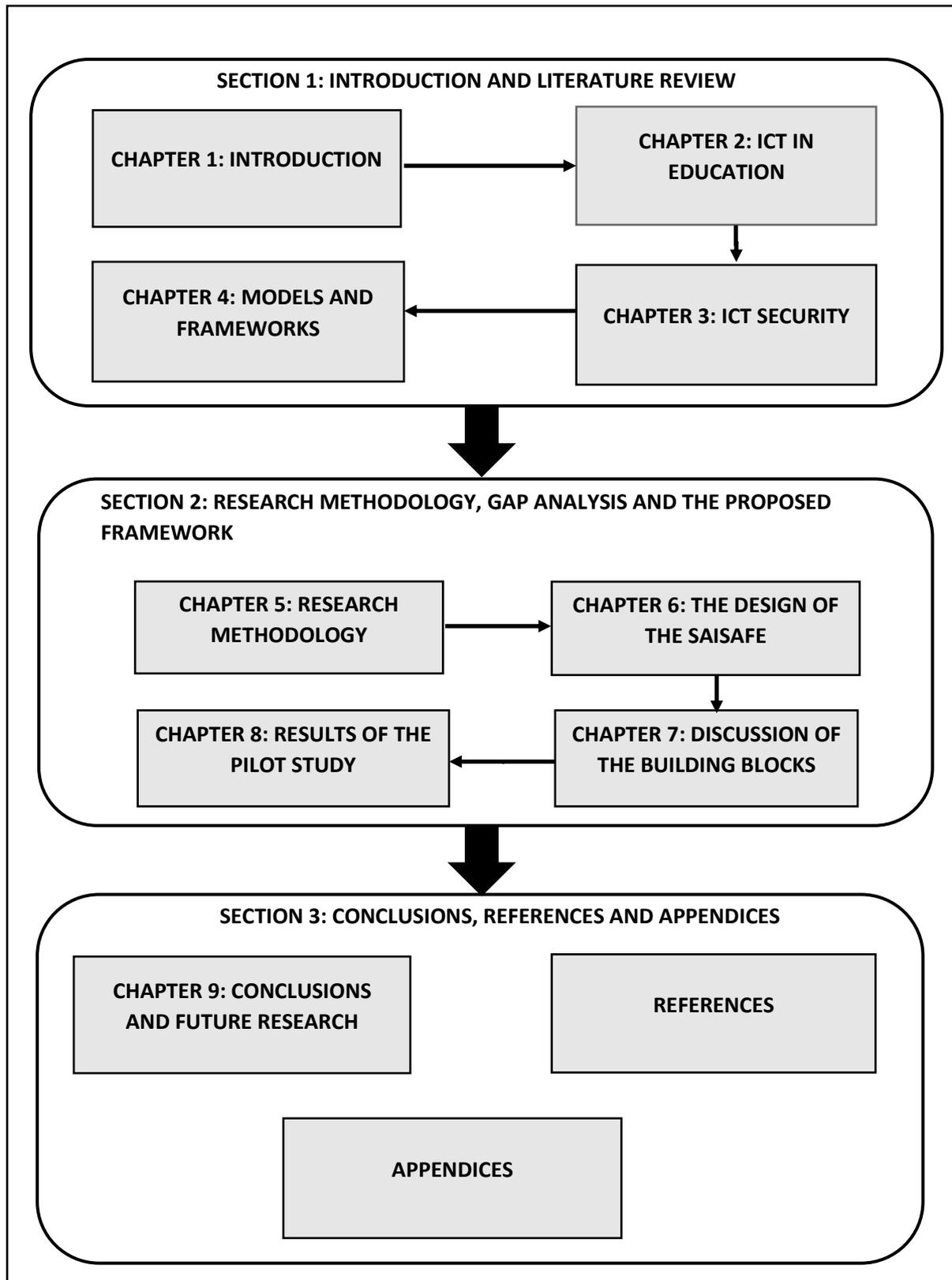
## 1.2.5 Structure of the Dissertation

Section 1 comprises Chapters 1 to 4, and contains the introduction, problem statement, research questions, objectives, methodology, deliverables, as well as the diagrammatic representation of the research process. A review of the literature consulted by the researcher was reported on in Chapters 2 and 3.

Section 2 comprises Chapters 5, 6, 7 and 8. Chapters 5 and 6 present a discussion of the research methodology that was used, the analysis of models and frameworks, and the design of the South African ICT Security Awareness Framework for Education (SAISAFE). The discussion of the building blocks of the proposed framework and the results of the pilot study are dealt with in Chapters 7 and 8 respectively.

Section 3 contains only Chapter 9, and it presents the researcher's conclusions and recommendations for future research. The thesis concludes with the references consulted and four appendices containing the researcher's articles that have been accepted for publication, as well as the questionnaire administered in this study.

In order to orientate the reader, a diagrammatic representation of the research process and the layout of this thesis is given next (see Figure 1.1).



*Figure 1.1: A Diagrammatic Representation of the Research*

## 1.3 Limitations and Scope of the Study

The limitations of this study include the scarcity of the research participants (ICT security experts) that can evaluate the viability of the proposed framework. Another limitation is the implementation of the proposed framework. Government institutions such as the Department of Education would need to adopt the framework so that it can be implemented and its viability tested in South African education. Given the complexities that are often associated with getting something legislated and adopted by the South African government, it would be challenging to get the Department of Education to adopt this framework in order for its viability and effectiveness to be tested.

This study is limited to the confines of the South African education system. It focuses on the integration of ICT security awareness into the South African schooling system and not anything other country. The study aims to propose for the integration of ICT security awareness into the South African schooling system from kindergarten up to and including the South African tertiary institutions both public and private.

## 1.4 Summary

Chapter 1 served as an introduction to the research and illustrated the background of the research. The problem investigated in this study involves the inadequate ICT security awareness of school learners in South Africa and ways of dealing with this shortcoming. The chapter also listed a number of questions that are pertinent to this research. One of the main research questions relates to a suitable framework that can be used to integrate ICT security awareness into the South African education system. The questions are linked to research objectives that have the overall aim of formulating and proposing a framework that is relevant for the education system in South Africa – the South African ICT Security Awareness Framework for Education (SAISAFE). A diagrammatic overview of the entire research process, which also depicts the layout of the thesis, is presented in Figure 1.1. Lastly, the limitations and scope of the study were outlined in Section 1.3.

# Chapter 2: ICT in Education

## 2.1 Introduction

The purpose of this chapter is to provide some background on the usage of Information and Communication Technology in education in South Africa and abroad, as well as to give the reader an idea of the level or amount of ICT usage in education in general. Its aim is to examine the usage of ICT in education, since ICT usage in any industry requires some level of ICT security awareness. A literature review of the state of ICT usage in education was consequently conducted.

By evaluating the usage of ICT in education in other countries, the researcher tried to give the reader some insight into what other countries have been doing in order to benchmark that against the usage of ICT in education in South Africa. It is important to first gauge the level of ICT usage in education in general, as it will then be possible to determine the amount of ICT security awareness that is needed in South Africa.

As in most industries, there are advantages and disadvantages of using ICT in education. These advantages and disadvantages, the challenges of integrating ICT in education, and lastly, the potential ICT security threats that are facing school learners are also discussed in this chapter.

## 2.2 ICT in Education

ICT in schools provides an opportunity for educators to transform and improve their teaching methods (PriceWaterhouseCoopers, 2010). ICT also provides educators with better educational content and more effective teaching and learning methods. Four key target areas can be identified for the improvement of education through ICT (Miller, Naidoo and Belle, 2003):

- Preparing learners and educators for using ICT technology
- Increasing learners' access to education
- Introducing new and spontaneous learning and teaching methods
- Improving class and overall school administration

People's participation in the usage of ICT is influenced by their attitudes, their confidence levels and their emotional styles (Maholwana-Sotashe, 2007). This statement implies that it depends on an individual's attitude and willingness to learn new technologies and integrate ICT in his/her teaching methods. Therefore, if these individuals (educators) are willing to learn new technologies and other ICT initiatives, then they will be willing to integrate ICT in their daily teaching methods.

It is important to occasionally benchmark what is being done in other countries against what we are doing in South Africa. A brief discussion about the usage of ICT in education in other countries and the usage of ICT in education in South Africa follows in the next sections.

## 2.3 ICT in Education in Other Countries

The usage of ICT in education in other countries is determined mainly by the state and level of their economies. For instance, in first-world countries like the United States of America, there is a significantly higher usage of ICT in education (Ford and Botha, 2010). When one compares that to countries like India and Kenya, there is still minimal usage of ICT in education in those countries, despite improvements over the years (Nyakowa, 2014). Researchers such as Mullamaa (2010) and Hong and Songan (2011) have conducted research relating to ICT in education in their respective countries, namely "*ICT in Language Learning - Benefits and Methodological Implications*" and "*ICT in the changing landscape of higher education in Southeast Asia*"

ICT in education is influenced by a number of factors. For instance, Lau and Albion (2010) state that, in Hong Kong, the usage of ICT in education is similar to that in other parts of the world because educators have a positive attitude towards ICT if it is used for preparation and administration, but not when it is used for the actual class work. Lau and Albion (2010) further report that there is a lack of time to incorporate technology in the class environment because this requires locating and previewing resources, as well as extensive planning.

In a developing country like India, there has been a significant increase in the use of ICT in education, as confirmed by Gundimeda (2014) in his research. However, Roy (2012) reveals that rural schools in India face many challenges when compared to their urban counterparts. Some of the problems mentioned by Roy (2012) are the following:

- The low salaries paid to educators in rural schools, resulting in educators neglecting their work.
- The lack of proper infrastructure which results in schools not having facilities such as computers.
- Lack of proper transport, which results in children being discouraged because they have to travel long distances to school.
- The relatively low level and standard of education in rural schools.

In the same way that technology has made inroads in production, consumption and distribution in the workplace, it is making an even greater impact in education (Qureshi, Raza & Whitty 2014). Social media is used extensively as a form of communication across the world. Based on their study, Qureshi et al. (2014) suggest that Facebook can be used as a learning tool in higher education institutions. Well-established countries that have good ICT infrastructure also make use of technologies like Facebook to improve learning at their institutions.

Because Facebook is widely used by many people across South Africa, it can be utilized by education institutions that offer long distance education (like Unisa) to disseminate information. This information can even include curriculum information, subjects, exams, and many more. This shows that ICT can be a useful tool for enhancing and improving education.

Having looked at the usage of ICT in education in Hong Kong, Kenya and India, it is evident that many of these countries experience challenges when it comes to the usage of ICT in education. The next section discusses the usage of ICT in South African education.

## 2.4 ICT Usage in South African Education

As a result of the advances in technology in South Africa, there has been a significant increase in the usage of ICT in education in the country. The growing usage of ICT in South Africa has prompted various higher learning institutions to take advantage of e-learning at their institutions (Moll, Adam, Backhouse & Mhlanga 2007). Because South Africa is one of the economically most diverse countries in the world, there are many factors that affect the usage of ICT in its education system.

South Africa has notable disparities when it comes to education in the country (Surty, 2011). The level and standard of education that is offered and received in private schools is different to the standard and level that is received and offered in public (government-funded) schools. With private schools having far more resources than the public schools, ICT is much more affordable for these institutions than the latter (Dlodlo, 2009). However, attempts have been made by the South African government to bridge the gap between private and public schools by giving schools in Gauteng computers, interactive whiteboards and tablets, and by putting up free WIFI in some schools (John, 2015). This has been seen as the right step towards bridging the technological gap and increasing the usage of ICT in education in South Africa.

Some educators in South African schools are still using ICT merely to transmit subject content rather than using it to improve their teaching and students' learning (Ndlovu and Lawrence, 2012). During the past two decades, the SA Department of Education realised that the need for the integration of ICT in education can no longer be ignored (Amedzo, 2007), and thus the Department of Education began including Information Technology (IT) in the curricula for the different school grades. In 2004 the Department of Education released a White Paper to facilitate the introduction of e-Education in South African schools.

Various academics and practitioners all over the world agree that the integration of ICT in education has a positive impact on the learning environment (PriceWaterhouseCoopers, 2010). Taking into consideration the diverse socio-economic and cultural backgrounds of learners, ICT can be used to reach an increased number of students, especially those who did not previously have access to quality education (especially in countries like South Africa). ICT can also assist to expose these students to various technical skills that are required in the job market.

Government institutions, the private sector and non-government organisations (NGOs) have come on board to assist schools with the task of integrating ICT in education. Examples of such institutions are Telkom (the Telkom Foundation), Microsoft South Africa (the Microsoft Foundation) and many others. Despite the intervention from these institutions, Amedzo (2007) notes that there is still a need for new technologies that will speed up the delivery of education and textbooks in rural areas to keep pace with such delivery in urban areas.

A number of South African tertiary institutions have introduced the use of ICT (Moll *et al.*, 2007). An institution like the University of South Africa (UNISA) makes use of emails to communicate with its students who are literally scattered all over the world. Other tertiary institutions also offer lectures over the internet and through other media (like Video-on-demand) for students who are situated at remote campuses. The increased usage of ICT in South African education has revealed and highlighted a number of advantages and disadvantages of using ICT in education. The next section discusses these advantages and disadvantages.

## 2.5 Advantages and Disadvantages of Using ICT in Education

While the integration of ICT in education has had a huge impact on revolutionising the global economy, it has also changed the traditional ways of teaching (Bushati, Barolli & Dibra 2012). Like many innovations, ICT may look all glamorous and good, but it has advantages and disadvantages that must be noted. The next section first looks at the benefits of ICT in education.

### 2.5.1 Benefits of Using ICT in Education

The usage of ICT in education has changed both teaching and learning domains. Several studies have shown that the usage of ICT in education has had a positive impact on learning when compared to instances where it is not used (Mikre, 2011). Bushati *et al.* (2012) list the following advantages of using ICT in education: ICT enables students to get better and effective education; ICT encourages individual study among students; ICT provides instruction according to the student's needs; ICT provides educational content and activities from diverse geographical areas.

According to Mikre (2011), the usage of ICTs in education simplifies the implementation of the curriculum and makes it learner-centred. It creates a self-learning environment and enables students to customise their learning experiences. ICT usage in education prepares students for the real world and provides teachers with new sources of information and knowledge. It improves communication and collaboration between students and teachers,

and creates greater enthusiasm for learning among students. Mdlongwa (2012) suggests that if ICT is implemented properly, then the following benefits of using ICT in teaching and learning can be expected:

- Increased collaboration and motivation among learners and educators
- Improved skills and knowledge among educators and learners
- Active participation in the classroom
- Increased responsibility and self-esteem

One of the benefits of using ICT as mentioned in the PriceWaterhouseCoopers (2010) paper is that the use of various multimedia devices (television, computer applications, etc.) can improve the learning process through the provision of collaborative educational material, which significantly increases learner motivation and enables learners to acquire basic skills. Mikre (2011) states that the usage of ICT in education changes students' learning approaches and an increase in activity and greater responsibility by the students has consequently been observed. The research further states that the usage of ICT in teaching can be of great assistance because simulated and individualised learning environments can be designed and constructed for learners. Another critical benefit of ICT usage in education is the increasing possibilities of innovation by learners when they use technology.

Using computers already from a young age helps students to learn ICT skills that can assist them as tools in their educational process. According to Miller et al. (2003), the following are some of the advantages of using ICT in teaching and learning:

- The usage of better equipment (such as multimedia) for learning
- Improved access to information (the use of the internet to get information)
- Improved learner response to learning (the inquisitiveness of learners during class)
- Skills development among both learners and educators (educators gaining new skills)
- More interesting teaching and teaching methods
- Better class management and administration

Even though ICT simplifies and facilitates human activities (such as communication, teaching and learning) in many respects, it also has limitations and disadvantages (Mikre, 2011). The disadvantages and limitations of using ICT in education are discussed in the next section.

## 2.5.2 Disadvantages and Limitations of Using ICT in Education

The limitations of ICT usage in education can be categorised as teacher related, student related, and technology related. Some of the disadvantages of ICT in education by different authors in literature in different countries are mentioned in the following paragraphs.

A notable limitation of ICT usage among school learners is the multiplicity of information available on the internet. Teachers have to spend considerable amounts of time trying to control what content the school learners are allowed to have access to in relation to learning content (Bushati *et al.*, 2012). Limitations that are mentioned by Mikre (2011) with regard to ICT usage in education mainly concern student behaviour:

- Computers can limit the student's imagination.
- Over-reliance on ICT limits critical thinking and analytical skills.
- Students lose the opportunity to use oral and hand-writing skills.
- An increase in the copying of school work from the internet (plagiarism).
- Physical side-effects such as vision problems.

According to Bushati *et al.* (2012), the following disadvantages and limitations when using ICT in education can be experienced:

- A so-called digital gap can be created by ICT among students, with some students being more comfortable with technology than others.
- ICT may deviate from the main goal of learning and end up having students more focused on ICT than on the actual learning of school work.
- Using ICT in the school context may eliminate the personal connection and relationship between a student and the teacher, as they could start using the technologies instead of face-to-face communication.

- Those teachers who are not technology literate can neglect their students and fail to update the content of courses.

Other disadvantages and limitations of using ICT in education include the lack of administrative support for the effective use of ICT; unavailability of appropriate content to offer to school learners; a lack of critical resources such as hardware, software and materials; and the administrative mandates to improve examination results (Fu, 2013).

As is normal when changes are implemented, challenges may be encountered when integrating ICT in education. Some of these challenges are discussed briefly in the next section.

## 2.6 Challenges of Integrating ICT in Education

The integration of ICT in education comes with specific challenges. Mikre (2011) states that the teacher's attitude plays a critical role when it comes to the usage of ICT in education. Research further states that even though attitude (a potential building block of this research) is vital, observations have shown that many teachers are not aware of the benefits of integrating ICT into the school curriculum.

Another challenge mentioned by Mikre (2011) is the misuse of technology by students. Instead of using ICT for learning purposes, students use technology for leisure activities such as online gaming, social networking (such as on Facebook and Twitter), and many more. Mdlongwa (2012) mentions the following as some of the challenges experienced with the implementation of ICT in schools:

- The high cost of technology implementation and maintenance. It is expensive to install and maintain software and hardware.
- Fear of change among educators and fearing that they will not cope with new technology. This may cause their work to be ineffective.
- The language used. Most software packages are written in English, which is not the mother tongue of most learners and educators. Inadequate proficiency in English can lead to ineffective use of the hardware and software.

Miller, Naidoo and Belle (2003) add the following to the challenges mentioned above: time (class preparation time, slow internet); inappropriate usage (learners accessing inappropriate content such as pornography and plagiarism); learners' writing skills (learners writing school work in SMS language, jargon and slang); diminished interest in other subjects (learners not interested in other subjects that do not involve technology). The challenges mentioned here are related to the integration of ICT in education as a whole. The next section below discusses the potential ICT security threats that face school learners within the education system.

## 2.7 Potential ICT Security Threats Facing School Learners

The section that follows discusses some of the most common ICT security threats that can affect school learners. These threats include inadequate cyber-security when browsing the internet, visiting social websites like Facebook and Twitter, and using instant messaging applications like WhatsApp and MXit.

### 2.7.1 Social Media

School learners nowadays make use of social networks to interact, as well as to improve their problem-solving and critical-thinking skills. This is done by sharing of school work, ideas, as well as solutions using these platforms. School learners can collaborate and discuss school work using social media platforms. They can also establish relationships and form study groups among each other to enhance their schooling using social networks.

Some of the most frequently used and well-known social websites used by school learners are Facebook and Twitter (Brownson, 2014). Various other social media platforms have also been created for school learners to interact, for instance, Brownson (2014) mentions a social website called Edmodo which is used for academic interaction within an academic environment.

Social media bring many benefits to an organisation, but at the same time they can cause serious security threats to it (Chi, 2011). In order for organisations to reap the rewards and

benefits that come with social media, they have to ensure that effective information security policies are in place and actively enforced. According to Communications Security Establishment Canada (2013), social media websites can pose a threat because these networks are frequently targeted by a wide variety of people attempting to gain access to information, projects, and systems.

### 2.7.2 Cyber-Crime

A significant number of cyber-crimes have occurred in South Africa in recent years. Of major concern is the fact that this number is increasing rapidly, instead of decreasing. Unfortunately, because of the lack of ICT security awareness, school learners are among the most vulnerable when it comes to cyber-crime.

According to Johnson (2012), cyber-crime costs the global economy huge amounts of money and causes major social and personal harm. Johnson (2012) further states that ICT security threats nowadays are increasingly diverse, unpredictable, and unforeseeable. Hence, it has become increasingly difficult for organisations and school learners to know how, when and why cyber-crime occurs.

Vermeulen (2014b) reports on an incident that occurred in South Africa where the SIM card of a person's mobile phone was illegally swapped and the person ended up being scammed of +-R5600 from his bank account. According to the website, no arrests have been made yet and the bank is denying liability for the scam. Vermeulen (2014a) also wrote about a new bug in the OpenSSL software library called "Heartbleed", which affected a number of South African (Bidorbuy and Capitec Bank) as well as global (Yahoo.com) websites.

The cyber-crime mentioned in the previous paragraphs has a huge potential to affect school learners, seeing that studies such as those by Kreutzer (2009) and MyBroadband (2014) show that school learners are among the highest users of ICT. The usage of ICT by South African school learners includes, but is not limited to, accessing social media sites (like Facebook and Twitter), instant messaging applications (like WhatsApp), and accessing the general websites. This usage has the possibility of exposing the school learners to cybercrime. This is one of the reasons why there have been calls for the inclusion of ICT security awareness in the South African school curriculum in order to educate school

learners about ICT security from an early age. According to the South African bill on cyber-crimes (Minister of Justice and Correctional Services, 2017), penalties can be imposed on anyone who is found guilty of offences related to cyber-crime in South Africa.

### 2.7.3 Instant Messaging

Since Instant Messaging (IM) is one of the technologies on which society relies for interaction and communication, it has become a vector for attacks (Poepjes and Lane, 2012). IM is a fast-growing means of communication that can be useful for both private and organisational usage. However, it can introduce a number of security risks if it is not properly managed (Liu, Shu and Lee, 2011).

### 2.7.4 Sexting and Exposure to Sexual Activities

Sexting is defined as the sending of naked or sexually suggestive pictures and messages using a mobile phone or instant messaging (UNICEF, 2012). As studies have shown that there is an increase in the usage of mobile phones among school learners in South Africa (Kreutzer, 2009), learners are at risk of falling victim to sexting. Smit (2015) reiterates the wide prevalence of sexting among school learners in South Africa and all over the world.

### 2.7.5 Social Engineering

According to Ahmad (Ahmad, 2012), social engineering is when someone is manipulated into giving out confidential information. As a result of their inadequate experience of using ICT, school learners may easily fall victim to social engineering.

### 2.7.6 Cyber-Bullying

Even though bullying existed before the existence of the mobile phones and the World Wide Web, these platforms have expanded the manner in which bullying can be executed (UNICEF, 2012). Cyber-bullying is any act of bullying that occurs through technology (Kritzinger and Padayachee, 2007). School learners can fall victim to this threat if they are not made aware of the dangers that come with ICT usage.

### 2.7.7 The 419 Scams

The 419 scam is a form of scam that preys on people over communication media (such as email) and it involves large amounts of money that the offender promises the victim (Internet Service Provider's Association, no date). Unsuspecting and uneducated school learners may fall victim to these scammers if they are not warned against them. Even though these types of scams usually target adults, it is important that school learners are also aware of them so that they can be better prepared to deal with the scams when they are targeted and are victims.

### 2.7.8 Bluesnarfing

Bluesnarfing is the act of stealing someone's information using a Bluetooth-enabled device. School learners' increasing usage of mobile phones that are Bluetooth-enabled, as reported by Kreutzer (2009), makes them vulnerable to this threat. ICT security awareness initiatives will play a major role in ensuring that school learners are well-equipped to deal with these threats.

Even though there might be challenges and disadvantages of ICT in education, there are also a number of benefits. These benefits are mentioned briefly in the next chapter.

## 2.9 Conclusion

The second and third United Nations Millennium Development Goals are about promoting gender equality and achieving universal primary education. Governments around the world have tried to universalise primary and secondary school education by introducing various programmes and schemes, but there are still problems when it comes to accessing quality education in order to achieve high educational goals. One of the aims of the current research is to investigate factors such as ICT security awareness that can assist in enhancing the quality of school education.

This chapter investigated the ICT usage in the education sector. Topics such as the advantages and disadvantages of ICT usage in education and ICT threats faced by school learners were discussed. The benefits of ICT usage in education as well as the challenges of integrating ICT into the education system were also presented.

# Chapter 3: ICT Security

## 3.1 Introduction

In the context of this study, the phrase ‘Education System’ refers to all kinds of schooling in South Africa. This includes, but is not limited to, all the public schools, private schools, home schools as well as community based schooling in the country. Basically, the South African education system in this study refers to all schooling from kindergarten up to and including tertiary institutions within the borders of South Africa. This study aims to address the content (ICT security awareness) of what the students are taught within the education system and not necessarily what the other aspects of it entail.

The problem statement in chapter 1 bemoans the non-inclusion of ICT security awareness in the South African education schools’ curriculum. In this study, curriculum refers to the academic content that is being taught in the education system in South Africa. This study therefore refers to the content that is prescribed by the South African government (Department of Education) to be taught or offered in the South African education system.

This study refers to ICT Security in its broader context, which include aspects such as the concepts of information security (confidentiality, availability, and integrity), cyber safety (cyberbullying, exposure to harmful content such as pornography), and physical safety (musculoskeletal discomfort, visual problems, and internet addiction). It also refers to aspects such as ICT security threats, ICT security standards some of which are discussed broadly in this study. All of these concepts fall under the definition of ICT security that is being referred to in this study.

This chapter marks the beginning of the literature review presented in this research. It investigates the various aspects of Information and Communication Technology (ICT) security in South Africa and around the world. Topics such as the primary concepts of ICT security and the countermeasures that can be used to curb ICT security threats are also investigated in this section. The ICT security standards that curtail ICT security threats are presented in more detail and Section 2.2 investigates ICT security in general.

A number of information security threats that exist in the world are discussed in detail in this chapter. According to Mueller and Fibikova (2012), the main reason for implementing information security is to ensure that an organisation’s confidentiality, privacy and integrity

is protected. This chapter also discusses the significance, necessity and importance of information security in the world, followed by information security awareness and the principles of information security. Some general standards of information security are discussed, but our attention is first focused on the state of ICT security in the world.

## 3.2 ICT Security in the World

A number of definitions of ICT are found in the literature, but the most meaningful one for this research is the one put forward by Gokhe: ICT is the technology that supports activities involving gathering, processing, storing, and presenting data and information (Gokhe, 2000). Fourie and McNamara (2008) define ICT as a means of communication and information manipulation and sourcing. They further state that ICT includes a number of technologies that are responsible for the electronic processing and transmission of information.

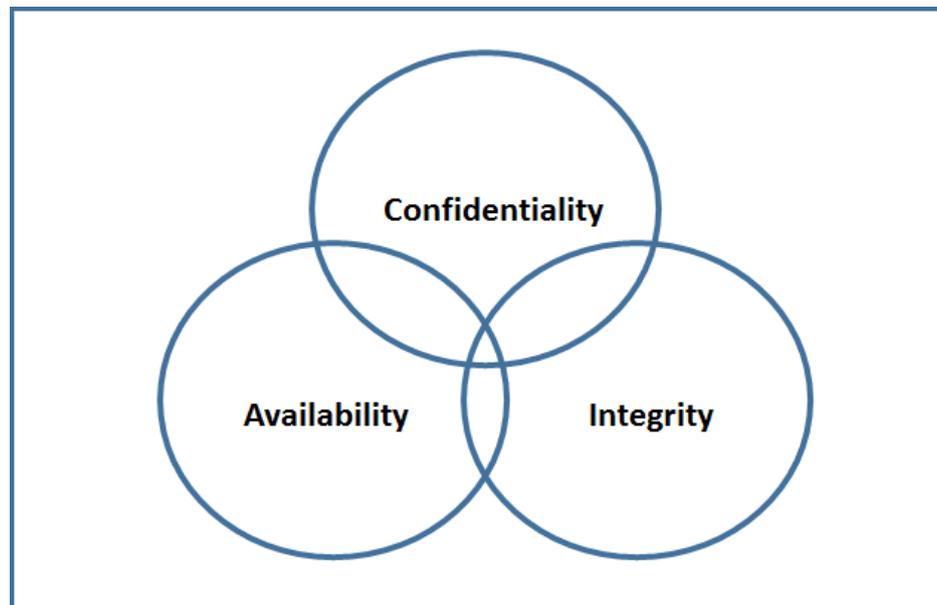
In a world where ICT has become vital and invaluable (The European Network and Information Security Agency (ENISA), 2010), ICT security has become increasingly important for the success of many businesses (Edwards, 2013). The increase in the prevalence of ICT-related crime globally has made ICT security an important resource in society. Research studies indicate that many people in developed countries use their laptops in coffee shops, they do internet banking on their mobile phones, and they shop online while sitting at home, using unsecured computers and networks. This obviously increases the risk of ICT-related crime harming unsuspecting users and it makes ICT security awareness a necessity.

ICT security is a broad subject that can be defined in a number of ways. According to Ashraf (2005), ICT security is the protection of information against fault, disclosure and manipulation. Verissimo and Rodrigues (2001) define information security as the confidentiality, integrity and availability of information. Andress (2011) states that information security is the protection of information and information systems from misuse, destruction, distortion and unauthorised access.

The literature review that was conducted as part of this research study revealed that there are many ICT security models and frameworks in the world (Walaza, Loock and Kritzinger, 2014). The three primary concepts of the majority of these models and frameworks are presented in Section 2.2.1.

### 3.2.1 The Three Primary Concepts of Information Security

The three primary concepts of information security – Confidentiality, Integrity and Availability – are commonly known as the CIA triad (Andress, 2011). The CIA triad provides a model (see Figure 2.1) that can be used when discussing information security concepts.



**Figure 2.1: The CIA Triad** (Andress, 2011)

The three primary concepts of information security are discussed briefly in the sections that follow.

#### Availability

Availability refers to the user's ability to access data as and when the need arises (Andress, 2011). Thus, data must be available at all times and whenever it is needed by its users. No unauthorised person or event should restrict access to information that should be commonly available (Information Security Resource Center, no date).

#### Confidentiality

Confidentiality of information is similar to data privacy, but it refers to the ability of the owner of the data to protect data from unauthorised access (Andress, 2011). Confidentiality involves ensuring that information is seen and accessed only by the people who are

authorised to do so. Some of the elements of confidentiality include the usage of strong passwords and shredding of documents (Information Security Resource Center, no date).

## Integrity

According to Andress (2011), integrity means that data is protected from being changed in an unauthorised and undesirable manner. The Information Security Resource Center (n.d.) specifies that data integrity requires that information may not be altered maliciously, in other words not intentionally, by natural disaster, and even by mistake. The three primary concepts above lead us to consider the ICT security standards that are needed to ensure them. According to Beckers et al. (2009) information security standards are introduced to establish a level of confidence for software vendors and provide information security assurance. Section 2.2.2 contains a brief discussion of ICT security standards in general.

### 3.2.2 ICT Security Standards

Security standards are used by software vendors to establish a high level of confidence for their products and to ensure that the assurance measures they have used are sufficient (Beckers, Heisel and Hatebur, 2009). The Government of the Hong Kong Special Administrative Region (HKSAR) (2008) states that an organisation can only benefit from information security standards if these are properly implemented. The HKSAR Government adds that all parties, from senior management down to IT professionals, have a role to play in securing an organisation. In this section various standards of information security are discussed briefly.

#### ISO Standards

The International Organization for Standardization (ISO) is a non-governmental international organisation that works with the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) on ICT standards (Government of the Hong Kong Special Administrative Region, 2008). Some of the commonly used and referenced standards are:

- ISO/IEC 27002:2005 (Code of Practice for Information Security Management)

- ISO/IEC 27001:2005 (Information Security Management System – requirements)
- ISO/IEC 15408 (Evaluation Criteria for IT Security)
- ISO/IEC 13335 (IT Security Management)

## Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard was developed by a group of major credit card companies to enhance the safe usage of cards for payment of accounts (Government of the Hong Kong Special Administrative Region, 2008).

## COBIT

According to Radovanovic, Radojevic and Sarac (2010), CobiT is an international standard that prescribes areas and individual controls for ICT governance, informatics and other related ICT processes. It combines business and ICT goals, and provides the ability to monitor the maturity of the information metric system. CobiT also enables management to optimise ICT resources such as applications, information, infrastructure and people (Radovanovic, Radojević and Sarac, 2010).

## ITIL (OR ISO/IEC 20000 Series)

According to the Government of the HKSAR (2008), the Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management and focuses on service processes of information technology.

One would have to use extensive measures to quantify the importance of ICT in South Africa. The importance, significance and necessity of ICT security for both organisations and individuals is discussed in the next section.

## 3.3 The Need for ICT Security

The significance and necessity of security in ICT is confirmed and augmented by the growing number of companies that are dependent on information technology (Alper, 2011). This growth affects not only companies, but also home users and school learners who are becoming increasingly dependent on ICT (Kreutzer 2009; Chigona & Chigona 2010). Ahmad

(2012) states that information security is essential to prevent and detect unauthorised access to one's computer system. Mueller and Fibikova (2012) advise that the following four areas should be taken into account when implementing information security:

- Information Users: how users handle information and tools to protect the organisation's information
- Business Processes: how information security is practised in day-to-day working
- Applications: whether applications are developed to ensure that information is protected
- Infrastructure: whether infrastructure is capable of handling unauthorised access to applications and networks in general

The four areas mentioned by Mueller and Fibikova (2012) prove that ICT security is crucial for organisations that make use of information technology. ENISA (2010) states that the reasons why an organisation may require information security awareness vary based on internal and external factors. The internal factors could be new technology implementation and new management, whereas the external factors could be new laws and a new government. According to Kabay (2002), the basic reason why people are concerned about information security is because their information needs to be protected from unauthorised access for legal and competitive reasons. The current research proposes that school learners should be equipped with the necessary knowledge to prevent unauthorised access to their information. Unauthorised access to information can be gained in a variety of ways, and some of the most common ICT security threats are presented in the section that follows.

### 3.4 ICT Security Threats

According to Andress (2011), a threat is something that has the potential to cause harm. The most common information security threats experienced by organisations and ICT users are discussed next.

### 3.4.1 Virus Threats

A computer virus is a program written intentionally to change or impede the normal operation of a computer system. It attaches itself to an existing program and then takes control via that program to access the computer that is being targeted (Whitman and Mattford, 2011). According to Ahmad (2012) a computer virus operates by replicating itself, thereby doing more and more damage to the system of the targeted computer.

### 3.4.2 Spyware Threats

Spyware is software that is installed or executed on a computer without the owner's knowledge and permission. According to Whitman and Mattford (2011), it is any technology that is used to gather information about a person or an organisation, without the permission or knowledge of the owner. Offenders use spyware software to monitor, track and report a user's movements to the spyware author, without the victim's knowledge (Ahmad, 2012).

### 3.4.3 Hackers

Hackers are people who use or create computer software to gain access to a victim's computer system without the latter's permission. A hacker looks to penetrate and exploit a weakness in a computer system or in an organisation's network (Whitman and Mattford, 2011). Offenders hack for many reasons for example to steal an organisation's confidential information (Ahmad, 2012), to make profit, to enjoy a challenge, or as some kind of protest.

### 3.4.4 Trojan Horse

A Trojan horse is similar to spyware but it is malicious software that is packaged and masked as another program – it only reveals its behaviour once it has been activated. It usually arrives as a harmless file or application with hidden malicious code embedded. A computer that has been attacked by a Trojan horse usually experiences system problems and loss of information (Whitman and Mattford, 2011).

### 3.4.5 Phishing Threats

Phishing occurs when offenders attempt to acquire a user's personal information by using communication media (a phone, email, instant messaging, fax, and many more) to steal the user's identity (Ahmad, 2012). Whitman and Mattford (2011) state that phishing attackers use three types of techniques – usually in combination with one another – namely URL manipulation, web site forgery, and phone phishing.

### 3.4.6 Pharming Threats

Pharming is the act of hijacking website addresses or URLs and redirecting an unsuspecting user to a fake website that looks like the original one. The fake website then collects all the information entered by the unsuspecting user and uses it for criminal activities. This kind of attack is also known as a Man-in-the-Middle (MITM) attack (Whitman and Mattford, 2011).

### 3.4.7 Adware and Advertising Trojans

Adware is software that delivers advertisements – such as pop ups and web links – without the permission of the computer owner (Whitman and Mattford, 2011). Adware is usually installed secretly through Trojans, but also through legitimate software that the owner has chosen to download and install. Adware can display advertisements based on the information collected by spyware that was already on the computer and that tracked the user's surfing habits (Ahmad, 2012).

### 3.4.8 Unsecured Wireless Access Points

A wireless access point is a device that allows wireless connectivity to a certain wired network using Wi-Fi or any other related standard. With so many devices being used these days to access the internet, wireless access points have also become threats to information security. Offenders often target unsecured wireless access points to gain access to private networks.

### 3.4.9 Social Engineering

Social engineering occurs when an unsuspecting person is manipulated into giving out confidential information (Ahmad, 2012). The confidential information gathered from the unsuspecting victim could be used for various reasons, such as unauthorised access to personal or organisational networks, online banking accounts, and many more. Whitman and Mattford (2011) argue that attackers are often some of the best social engineers because they have the ability to convince people to disclose important and highly confidential information.

Section 2.4 discussed only a small percentage of the prevailing ICT security threats – a vast number was not even mentioned. The threats mentioned can be dangerous and harmful, but fortunately there are countermeasures that can be used to safeguard the user against them. These measures are further discussed in the section that follows.

## 3.5 Countermeasures Against ICT Security Threats

ICT security threats can be countered to minimise or at least reduce their impact. The primary countermeasures that can be used against ICT security threats are classified under prevention, detection and reaction (Veríssimo & Rodrigues 2001; Ahmed 2012). Besides these basic methods, three more countermeasures – identification and authentication, authorisation and access control, and information security awareness – can be used to curb ICT security threats. All of these countermeasures for safeguarding a system against falling victim to an online security attack are presented briefly in the subsections that follow.

### 3.5.1 Prevention

Verissimo and Rodrigues (2001) state that prevention refers to the inhibition of security violations and the enforcement of access controls. Ahmad (2012) describes prevention as doing everything possible to keep information security threats at bay.

### 3.5.2 Detection

Detection refers to the prompt detection of security violations and system failures, and taking speedy action to alert defenders (Ahmad, 2012). Detection comes into play when prevention measures have failed or have been exhausted (Veríssimo and Rodrigues, 2001).

### 3.5.3 Reaction

Reaction refers to the situation that arises when a security violation occurred. Ahmad (2012) believes that detection has minimal value if one does not have the ability to respond. Verissimo and Rodrigues (2001) state that reaction methods may vary, depending on the area that was violated. Though reaction is listed as one of the first measures to be taken against information threats, information security managers should not spend too much of the time reacting. Reacting can limit the opportunity to figure out the root causes and finding longer-term solutions to problems (ISACA, 2009).

### 3.5.4 Identification and Authentication

A well-written information system connected to a network should be configured in such a way that it is able to uniquely identify and authenticate end user operated devices. According to Andress (2011), identification is the process of confirming who a person or system is claiming to be. This can include a couple of scenarios, for instance asserting the original source of an email by using usernames, DNA samples, fingerprints, etc. Andress (2011) further states that an uncorroborated claim of identity cannot be accepted as reliable proof of security on its own, hence the need for authentication.

In the information security context, authentication is a set of methods that are used to check whether the claim of identity is true or not. Authentication only verifies the claim of identity and does not examine what the authenticated party is allowed to do on the system or network (Andress, 2011). A password to log into a computer and entering a PIN at the ATM are good examples of authentication. The different levels and types of authentication methods, however, fall outside the scope of this research.

### 3.5.5 Authorisation and Access Control

After the claim of identity and authentication has been established, the next step in curbing security violations is authorisation and access control. Andress (2011) argues that authorisation enables one to determine what users are allowed to do and what they are not allowed to do. Furthermore, Andress (2011) describes four tasks that are carried out when

access controls are implemented, namely allowing access, denying access, limiting access, and revoking access.

### 3.5.6 Information Security Awareness

Information security awareness can play a major role when it comes to reducing the impact of ICT security threats. In fact, Kruger and Kearney (2008) believe that information security initiatives and programs are key defences against security incidents. According to Kritzinger and von Solms (2010), it is important that all users of the internet are aware of the dangers associated with its use.

In their study, Adedayo and Ayobami (2013) found that information security awareness has a clear impact on information security threats in the student community. Kritzinger and von Solms (2010) emphasise the importance of information security awareness by proposing an E-Awareness model that can be used by all people who make use of the internet. These studies prove that the knowledge of users with regard to information security can be greatly enhanced if there are information security initiatives and programs in place. A more in-depth discussion of ICT security awareness is presented in the next section.

## 3.6 ICT Security Awareness

ICT security awareness is an attempt to change the technology and internet usage behaviour and patterns displayed by employees of organisations and the general public (The European Network and Information Security Agency (ENISA), 2010). Ashraf (2005) reckons an organisation may have the best information security awareness program in place, but if it does not manage its resources in a proper manner, it will not be able to complete and implement that program successfully.

ICT security awareness is important because we live in a world where ICT has become a part of the everyday lives of millions of people (Kritzinger and Von Solms, 2010). ICT is not only used by businesses, organisations and government departments for work purposes, but also comprehensively by home users for doing shopping online, online banking, communicating (email), searching for information and many more. This exposes users and renders them vulnerable to some (if not all) of the security threats that were mentioned in Section 2.4.

Kritzinger and Von Solms (2010) state that the vulnerability experienced by home users is caused by their lack of knowledge on how to protect themselves against ICT security threats.

According to Poepjes and Lane (2012), a lack of information security awareness characterises many organisations and society in general. To emphasise the importance of information security awareness; Kritzinger (2006) goes as far as saying that employees of an organisation cannot be held accountable for information security breaches that occur if they have not been made aware of the importance of securing the information they work with.

The fact that it is not only a disadvantage, but actually dangerous for school learners to be able to use a variety of modern technologies while being unaware of ICT security (Rowe, Lunt & Ekstrom 2011), confirms the importance of this research and further emphasises the need for ICT security awareness in education. The impact and seriousness of this danger is evident when Rowe et al. (2011) state that many academics have insisted that cyber-security be included in the school curriculum.

The research in hand focuses mainly on South African school learners, and the need for effective ICT security awareness among school learners is emphasised in the following section.

### 3.6.1 The Need for Effective ICT Security Awareness among School Learners

A significant number of ICT-related cases of crime occurred in the past couple of years (Belayneh, no date). Research has shown that most ICT-related crimes occur as a result of the lack of ICT security awareness of end users (Kritzinger and Von Solms, 2010). Aloul (2012) further observes that ICT security awareness is often overlooked by organisations when they implement their ICT security programmes. It is for these reasons (among others) that this research deems it imperative that learners should be made aware of ICT-related crime already during their schooling years, as it will equip them to deal with ICT-related crime as and when necessary. In fact, the huge increase in ICT usage by school learners makes ICT security awareness an immediate necessity.

Nowadays, computer use by school learners is common in many countries and internet exposure varies with the types of technologies available, age, gender, and social group (Straker, Pollock & Maslen 2009). In a study conducted by Kreutzer (2009), it was found that school children use the internet and mobile phones not only for academic purposes, but also (and especially) for activities such as communication, entertainment, visiting websites, and instant messaging. Kritzinger and Padayachee (2007) therefore state that it is important and beneficial for school learners to be taught about ICT security at an early age.

The amount of usage of ICT by school learners exposes them to a number of serious dangers (for instance child-trafficking) and security risks. According to Kritzinger and Padayachee (2007), children are also exposed to security and safety issues such as identity theft and computer viruses. Excessive and unsecured use of ICT devices can even affect children physically and mentally – carpal tunnel syndrome and cyber-bullying respectively come to mind as some of the issues that can affect children when using ICT devices. Researchers in South Africa and around the world have done extensive work by proposing models and frameworks that are related to ICT security awareness.

Besides the ever-increasing ICT-related crime occurring in industry, many other dangers face school learners when they use ICT. For example, perpetrators make use of the internet, social media platforms, instant messaging and many other ICT platforms to entice young children into pornography (Nevondwe and Odeku, 2014). On these platforms, learners face the risks of child trafficking, paedophilic attacks, and many other criminal elements. Unmonitored access to the internet also makes school learners vulnerable to general ICT-related crime. These crimes and risks will be minimised if school learners are made aware of ICT security. Lack of ICT security awareness among school children is not a problem only in South Africa; it is a global issue. However, for the purposes of this research, the next section discusses ICT security awareness with a focus on South African organisations.

### 3.7 ICT in South Africa

According to Gillwald, Moyo and Stork (2012) South Africa has the characteristics of both a developing and an advanced economy when it comes to ICT. South Africans have access to many technologies, research institutions, universities, private companies and governmental

organisations that have good resources. However, more than half the population still live in poverty and huge anomalies are clearly evident in the South African ICT sector (Gillwald et al. 2012).

A former South African minister of communications, Yunus Carrim, stressed the importance of Information and Communication Technology (ICT) in developing the country's economy and reducing the inequalities of our societies (Department of Communications, 2014). The White Paper published by Bell ICT Solutions (2007) further stipulates that ICT can assist through education by creating a more sustainable and accessible learning environment that will result in teachers and learners enjoying an improved and richer learning experience.

Significant growth occurred in the ICT sector in South Africa over the last two decades (Gillwald, Moyo and Stork, 2012). In 2014 there were two fixed-line operators (Telkom and Neotel), five mobile operators (Vodacom; Cell C; MTN; Telkom Mobile, Virgin Mobile), and hundreds of internet service providers (ISPs). The ICT sector currently contributes significantly to the GDP of the country. Even though much improvement has been made, the South African ICT sector is still ranked poorly in global ICT indices (Gillwald, Moyo and Stork, 2012). According to Venktess (2016), South Africa dropped from 86 to 88 in world rankings on the global ICT indices in 2016.

The South African Department of Communications (DoC), which is one of the custodians of ICT in the country, published a Green Paper in which it states its purpose as having to change and improve the ICT sector and the country's economy (Department of Communications, 2014). It decries the fact that the country has not yet taken advantage of the possibilities and opportunities that are created by the digitisation and convergence of communication technologies. According to the DoC's Green Paper, the communications industry in South Africa is divided into telecommunications, broadcasting, and postal services (Department of Communications, 2014).

Gillwald et al. (2012) believe that ICT usage in South Africa is often characterised by the disparities in classes within the country, with the high income earners being more readily exposed to technology than low income earners. Like in other developing countries, there is a slower adoption of ICT in the public sector, even though this sector represents the majority of the population. With these inequalities in mind, the Department of

Communications (2014) noted the high prices that South Africans are paying for basic communications, compared to other countries where people have been enjoying higher internet speeds at cheaper rates in the last decade. Gillwald et al. (2012) state that even though there are countless people who live below the breadline in South Africa, the effective social grant system assists many of them to have access to communication services.

As discussed in the previous paragraphs, ICT security awareness can play a major role in improving the economy and well-being of a developing country like South Africa. The next section discusses an important aspect of the usage of ICT, namely awareness.

### 3.7.1 ICT Security Awareness in South Africa

The usage of ICT across various industries has boosted the South African knowledge economy, which is essential for negotiating with global societies (Gundimeda 2014). Considering the highly increased ICT usage locally (Dlamini and Modise, 2012), it is evident that ICT security awareness is of utmost importance and, if ignored, it can pose a serious threat to the national security of South Africa (Dlamini & Modise 2012; Grobler et al. 2011). Dlamini and Modise (2012) claim that South Africa is one of the top three countries that have been targeted for phishing attacks. This has caused relevant institutions to embark on initiatives aimed at empowering South African citizens.

According to Drevin, Kruger and Steyn (2007), introducing ICT security awareness initiatives can make a significant contribution to the effectiveness of an organisation. However, Drevin et al. (2007) believe that effective security controls can only be achieved if employees of an organisation are made aware of the importance of information security. It is essential to evaluate the effectiveness of the current ICT security awareness initiatives in South Africa (Dlamini and Modise, 2012), and the local custodians of ICT need to embark on effective initiatives and campaigns that will enhance ICT security awareness among South African citizens.

Research studies show that a number of ICT security awareness initiatives have been launched in South Africa. Even the South African government has played its role to protect its citizens against cyber-crime by introducing the Electronic Communications and

Transactions (ECT) Act and the National Cyber Security Policy (Department of Communications, 2010). South Africa also promulgated a bill dealing with cyber-crimes and cyber-security (Minister of Justice and Correctional Services, 2017). South African academic institutions such as the NMMU, UNISA and the UFH have introduced their own ICT security awareness initiatives (Dlamini and Modise, 2012), and scholars from these institutions have also written a number of papers about ICT security awareness. Even the private sector (such as banks) formed institutions like SABRIC with the aim of equipping ordinary citizens and protecting the interests of the country. This proves that there is sufficient information and policies available about ICT security awareness in South Africa – the problem is adherence to and the implementation of these policies.

According to Belayneh (n.d.), a major problem faces South Africa when it comes to ICT security and drastic measures need to be taken. Craig Rosewarne (founder of ISG Africa), as cited by Kayle (2011), states that South Africa is lagging behind as far as ICT security awareness is concerned, compared to both its African and international counterparts. Craig Rosewarne further warns that South Africa does not have an incident response team that the whole country can use, and he stresses the importance of forming partnerships to deal with cyber-crime in the country. Belayneh (n.d.) goes on to mention a number of facts about ICT security in South Africa and specific incidents that occurred in the country in recent times.

- South Africa is in the top five countries regarding the highest number of victims of cyber-crime in the world.
- Most online technology users are unaware of how to protect themselves against cyber-crime and malware in South Africa.
- Some East Europeans started an illegal business and stole ±R50 million worth of airtime from MTN in South Africa.
- In May 2013, a huge amount of money was stolen from an Absa bank account belonging to the CEO of Media24.
- Statistics SA data shows that criminals are now targeting ordinary citizens to execute their attacks.

- Since there is no law that forces organisations that have suffered from cyber-attacks to reveal the details of such attacks to the authorities, it is difficult to measure the extent or frequency of cyber-attacks in the country.
- The citizens of South Africa feel helpless because the institutions that have fallen victim to cyber-crime (mostly banks) are denying liability and putting the blame on clients.

During their research, Walaza et al. (2014) studied a number of models and frameworks as part of their literature review and they conducted an analysis of these models and frameworks in order to propose a framework. Two of these models and frameworks (the ISRA model and the Teacher Development Framework) are from research studies done in South Africa. A number of scholars did research for proposing models and frameworks that are related to ICT security awareness in South Africa; for instance, Kruger, Drevin and Steyn (2006) proposed a framework for evaluating ICT security awareness. Kyobe (2010) also proposed a framework for guiding compliance with information system security policies and regulations at a university.

The frameworks and models in South African literature are focused not only on academia, but also on the private sector. For instance, Smith and Kruger (2010) proposed a framework for evaluating information technology security investments in a banking environment. Chetty and Coetzee (2010) proposed a framework for information security in the service-oriented architecture. The proposal of the ISRA model also emanates from research that was conducted in South Africa. These models and frameworks are an attempt to increase ICT security awareness among ICT users and to minimise ICT-related crimes as much as possible.

Four basic safety and security concerns for children have been identified with regard to ICT usage (Kritzinger and Padayachee, 2007), namely information security risks (malware, identity theft, etc.); physical risks (musculoskeletal discomfort, visual problems, etc.); personal social impact risks (withdrawal, internet addiction, etc.); and interaction threats (internet predation, cyber-bullying, etc.). Because of these issues and concerns and the growing usage of ICT by school children in South Africa, Kritzinger and Padayachee (2007) suggested the inclusion of e-safety and information security in the South African school

curriculum. Hence, we now look at the ICT security awareness situation in South African education in the next session.

### 3.7.2 ICT Security Awareness in South African Education

The number of internet users and Internet Service Providers (ISPs) has grown exponentially in the last number of years in South Africa (Kritzinger and Padayachee, 2007). Among this huge amount of internet users are school learners who do not necessarily have the skills and knowledge to protect themselves against ICT-related crime. Various interventions have been made by the South African government, such as the introduction of the National Cyber Security Policy (Grobler, Vuuren and Leenen, 2012), but these interventions do not guarantee the security and safety of school learners. Most South African learners remain vulnerable to ICT-related crime and this necessitates vigorous ICT security education and awareness directed specifically towards learners at school.

During a study conducted in South Africa about the usage of ICT devices (such as mobile phones) by school children in lower-income areas, it was found that 97% of the respondents owned mobile phones (Kreutzer, 2009). This statistic implies that an enormous number of South African school children are using ICT for interaction and communication. Given the vulnerabilities of children and the dangers they face on a daily basis, it is important to ensure their safety and security when they embark on this journey of ICT.

As mentioned by Rowe et al. (2011), it is far from ideal for school learners to have minimal knowledge and awareness of ICT security, given the number of technologies used nowadays. In many academic institutions school learners do their work (assignments and projects) on desktop computers that are connected to the network and internet. If these resources were unavailable, it may lead to loss of work and to schoolwork not being completed on time (Drevin, Kruger and Steyn, 2007).

Like any other type of business, academic institutions rely heavily on ICT resources for their day-to-day operations (Drevin, Kruger and Steyn, 2007). They therefore need to ensure the reliability, availability and confidentiality of their data at all times, otherwise productivity will decrease and their reputations will be seriously compromised. Some South African

academic institutions (like the University of South Africa) make use of networks to send academic material such as study material and assignments to students. Since they also use these networks for communication purposes on a regular basis, there needs to be an acceptable degree of ICT security awareness among school learners and staff. If this is not in place, these institutions are vulnerable and run a serious risk of falling victim to ICT-related criminal activities.

## 3.8 Conclusion

The prevalence of ICT-related crime (such as cyber-crime, 419 scams, and many more) stresses the great significance of ICT security awareness. The increase in ICT usage all over the world also plays a critical role in the increase of ICT-related crime and reiterates the important role of ICT security awareness.

This chapter looked at the current state of ICT security in the world and discussed the primary concepts of ICT security awareness and ICT security standards. The need for ICT security was stressed and various ICT security threats were highlighted.

Attention was also given to the countermeasures that can be used against ICT security threat, and ICT security awareness was discussed extensively. Lastly, the chapter contains a section that looked at the overall ICT security situation in South Africa as well as ICT security awareness in our education system. Chapter 3 will next investigate the use of ICT in the education system.

# Chapter 4: Models and Frameworks

## 4.1 Introduction

The models and frameworks that are presented in this chapter are divided according to two spheres: ICT security awareness and ICT in education. Many ICT security awareness and ICT-in-Education models and frameworks exist in the world (Ope, 2014), and in South Africa a number of these models and frameworks have also been proposed (Walaza, Looock and Kritzinger, 2015). The research in hand examined various models and frameworks (in both ICT security awareness and ICT in Education) with the aim of proposing a desired framework. It also identified building blocks that would be used when constructing the proposed framework. The term building block refers to components within the selected models and frameworks which are relevant to this research. These components are identified and considered for addition to the completed proposed framework.

Chapter 4 presents the models and frameworks that were used to construct the framework proposed in this research. These models and framework, which were chosen based on an in-depth literature review, are closely related to the topic of this research and represent the two spheres of ICT security awareness and ICT in education. The ICT security awareness models and frameworks that were presented are the Business Model for Information Security, the Information Security Retrieval and Awareness (ISRA) model, and the Comprehensive Information Security Framework (CISF). The ICT-in-Education models and frameworks are the Four In Balance model, the Teacher Development Framework, and the Model For ICT Rural Education.

A thorough review of the literature on the research topic was conducted and the researcher conducted an analysis of a number of ICT security awareness and ICT-in-Education models and frameworks. The following criteria were used to select the models and frameworks to be used:

- The relevance of the model or framework to the topic of this research
- The potential of the components of the model or framework to be used as building blocks in the proposed framework

- The relevance (or close relationship) of the model or framework to the South African context

The reason why many models and frameworks were discarded is that they were not relevant to the South African context. Another reason is that they did not offer any relevant building blocks that could potentially be used in the proposed framework. Based on an extensive literature review, some were found to be neither relevant nor related to the topic of this study. Rigorous selection criteria were applied to select the right models and frameworks, and the review of previous scholarly work related to the topic played a major role in this decision-making process. In the end, only the most suitable models and frameworks were chosen.

The two spheres of ICT security awareness and ICT in Education were chosen specifically because of their potential to enhance knowledge and increase ICT security awareness among South African school learners. A number of researchers such as Von Solms and Von Solms (2014), De Lange and Von Solms (2013), and Kritzinger and Padayachee (2007) mentioned the importance of teaching school learners ICT security at a young age to enable them to become ICT security-aware citizens in the future. Sections 4.2 and 4.3 present the selected ICT security awareness models and frameworks and the ICT-in-education models and frameworks.

## 4.2 ICT Security Awareness Models and Frameworks

The researcher selected a number of models and frameworks to be used as a basis for the proposed framework. This section investigates the ICT security awareness and ICT-in-Education models and frameworks that he selected from the available literature, namely:

- Business Model for Information Security (BMIS)
- Information Security Retrieval and Awareness (ISRA)
- Comprehensive Information Security Framework (CISF)

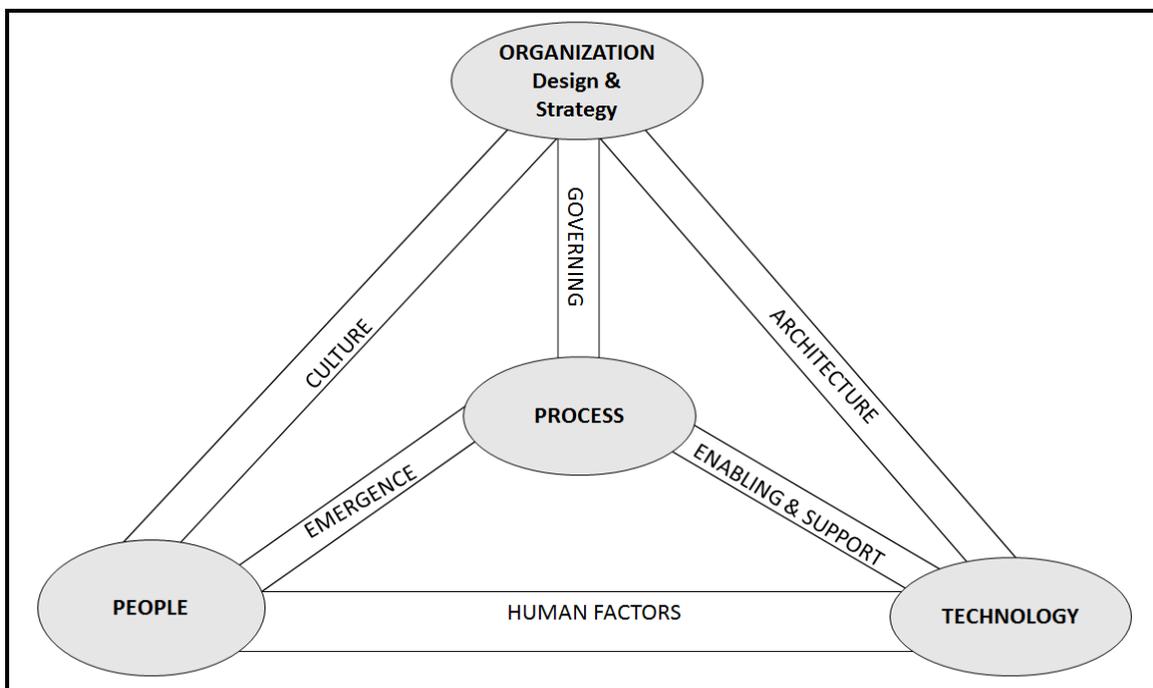
Although many other ICT security awareness models and frameworks exist in literature, the illustration and discussion of these models and frameworks in the subsections below is an

attempt to justify why these three were chosen and used in this research as the basis of the proposed framework.

#### 4.2.1 The Business Model for Information Security

The Business Model for Information Security (BMIS) is a model that gives guidance to people, process, organisation, and technology about ICT security awareness aspects. According to ISACA (2009), the BMIS can be used in all types of enterprises and would be compatible with all ICT security awareness frameworks that already exist in an enterprise. This model addresses ICT security awareness aspects that arise from poor governance, a dysfunctional or non-existent security culture, and employees who have not been trained about ICT security awareness. The BMIS is a practical tool that can be used to connect ICT security with business strategy (ISACA, 2009).

As depicted in the diagram in Figure 4.1, the BMIS consists of four components, namely Organisation, People, Process, and Technology. The building blocks that will be taken from this model are People and Technology.



**Figure 4.1: The Business Model for Information Security** (ISACA, 2009)

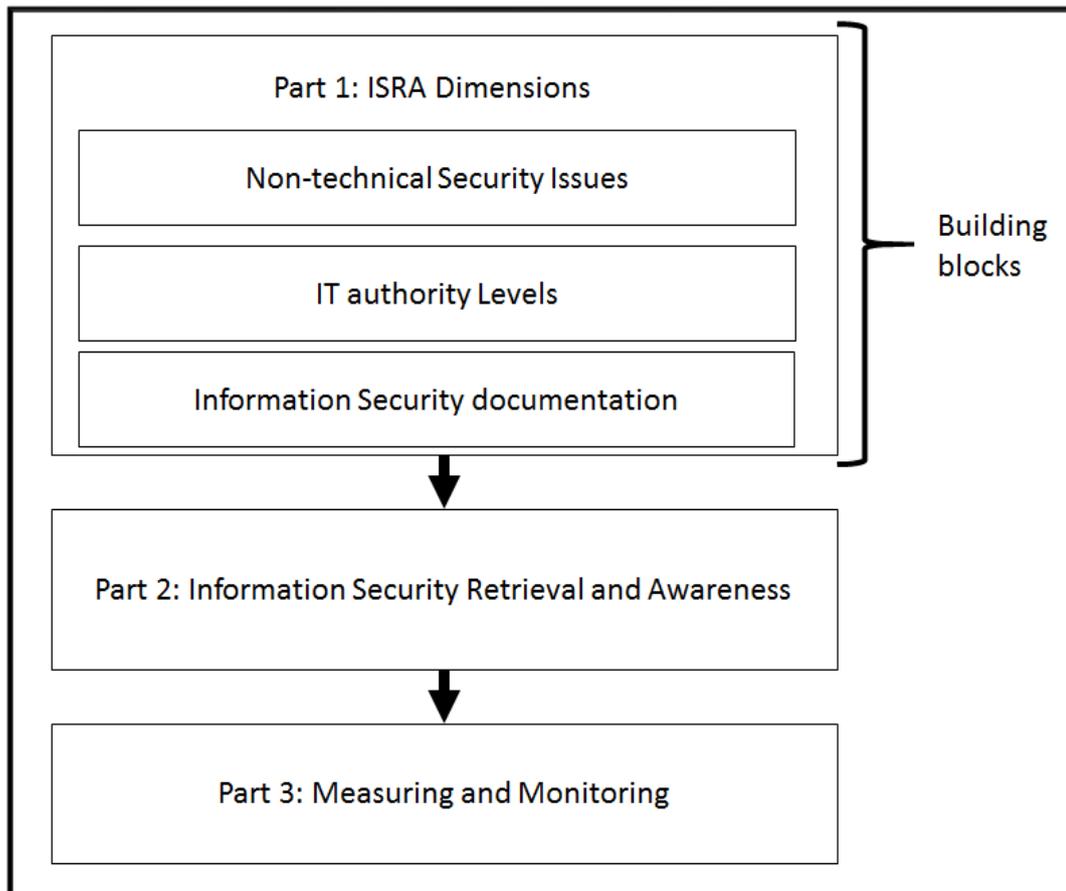
According to ISACA (2009), the Business Model for Information Security takes a business-oriented approach to managing information security. The model can be used in any type of enterprise, no matter the size of the organisation, whether it is technology independent, and whether is applicable across industries, geographies, and governing laws.

This model consists of components that are relevant to the theme and direction of the current research, namely people (enabling and support, human factors, governing, culture), and technology. Hence they will be used as building blocks during the formulation of the model proposed in this research. The fact that the model can be used in any type of enterprise is of vital importance and can be useful to this research.

#### 4.2.2 The Information Security Retrieval and Awareness Model

The Information Security Retrieval and Awareness (ISRA) model was developed specifically for the global ICT industry (Kritzinger, 2006). It ensures that stakeholders are made aware of the ICT security issues that are relevant to their specific job categories, and it does not burden them with information that is not relevant to them. Kritzinger (2006) states that the ISRA model allows stakeholders to retrieve information specific to ICT security awareness at any time. This can be useful to school learners who might need to access ICT security awareness information at different times in their lives.

The ISRA model consists of three main parts and its main focus area is information security awareness (Kritzinger, 2006). This is in line with the current research and the ISRA model will therefore be used extensively when proposing a framework for this research.



**Figure 4.2: The ISRA Model** (Kritzinger, 2006)

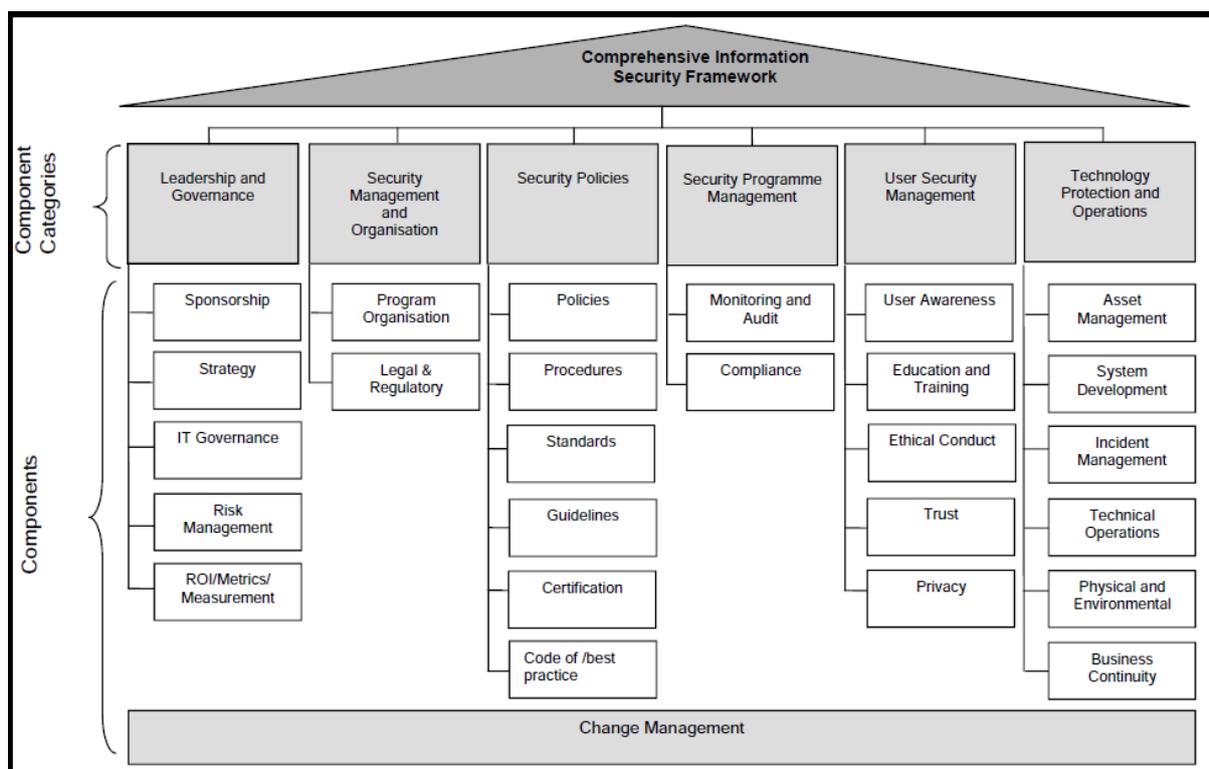
According to Kritzinger (2006), the main aim of the ISRA model is to enhance the information security awareness of employees in an organisation. As depicted in Figure 4.2, Kritzinger (2006) states that the ISRA model consists of three main parts, namely the ISRA Dimensions, Information Security Retrieval and Awareness, and Measuring and Monitoring. The building blocks that were identified from the ISRA model are information security documentation, and measuring and monitoring. These components are important in the South African context and will be used in the formulation of the proposed framework. The ISRA model aims to assist with the enhancement of information security awareness in South African education.

### 4.2.3 The Comprehensive Information Security Framework

The Comprehensive Information Security Framework (CISF) is a broad framework that can be used in different types of environments, which is why it was identified and used in this research. The CISF is structured under six component categories, namely Leadership and

governance; Security management and organisation; Security policies; Security programme management; User security management; and Technology protection and operations (Da Veiga, 2008).

The CISF contains components that can be used to formulate the framework proposed in this research. The components that were identified as building blocks are leadership and governance, policies, code of best practice, user awareness, and compliance.



**Figure 4.3: The Comprehensive Information Security Framework (Da Veiga 2008)**

The ICT-in-Education models and frameworks that were found in literature are discussed thoroughly in the next section. Some of these models will be used as building blocks to formulate the outcomes of the current research.

### 4.3 ICT-in-Education Models and Frameworks

There are many ICT-in-Education models and frameworks that exist in literature. Researchers such as Ford and Botha (2010), Plessis and Webb (2012), and many others proposed models and frameworks that are related to the ICT-in-Education sphere.

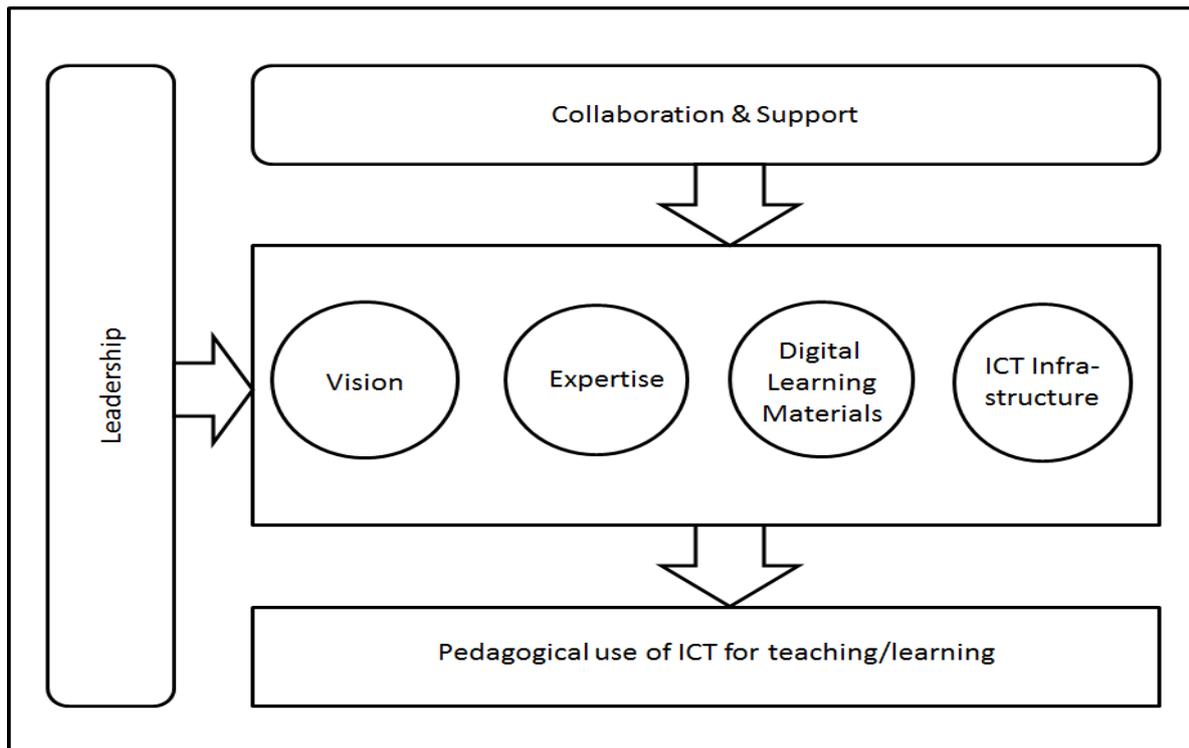
This section presents the ICT in Education models and frameworks that were chosen from the available literature to be used in this research. These models and frameworks will also be used as the building blocks for the proposed framework. The ICT in education models and frameworks that were identified as appropriate models and frameworks related to this research are the following:

- Four In Balance Model
- Teacher Development Framework
- Model for ICT Rural Education

These models and frameworks are discussed in the next paragraphs.

### 4.3.1 The Four in Balance Model

The first model selected in the ICT-in-education sphere is the Four in Balance model. Draper (2010) proposes the use of this model, which states that the use of ICT in education requires four basic elements: vision; expertise; digital learning materials; and ICT infrastructure. ICT adds value to the teaching and learning methods when these four elements are in balance (Draper, 2010). The Four In Balance model is depicted in Figure 4.4.

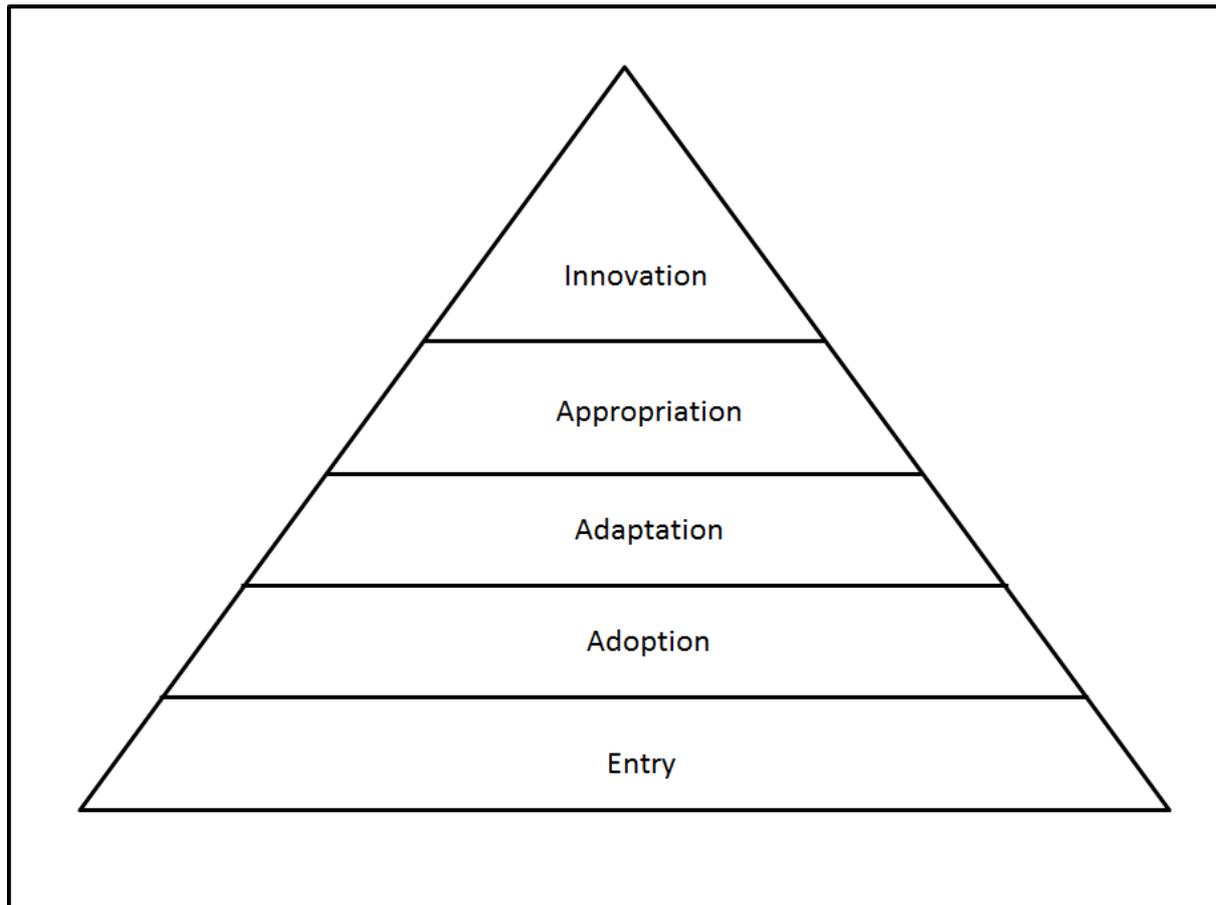


**Figure 4.4: The Four in Balance Model (Draper 2010)**

Of the four aspects presented in this model, Draper (2010) ranks Expertise as of highest importance. The model reveals that teacher expertise is the skills and knowledge required for the usage of ICT (Draper, 2010). *Collaboration and Support* and *Digital Learning Materials* were identified as building blocks that could be used in the construction of the framework for this research. The literature review that was conducted also revealed a lack of Collaboration and Support and of Digital Learning Materials as being related to ICT security awareness in South African education. Both of these building blocks meet the selection criteria and they fit in perfectly as components of the framework proposed in the current research.

### 4.3.2 The Teacher Development Framework

The Teacher Development Framework can be used for the training and the development of educators in ICT (Department of Education 2007; Ndlovu & Lawrence 2012). This framework comprises of the various levels such as Entry, Adoption, Adaptation, Appropriation, and Innovation. The Teacher Development Framework is depicted in Figure 4.5.



**Figure 4.5: The Teacher Development Framework** (Department of Education 2007)

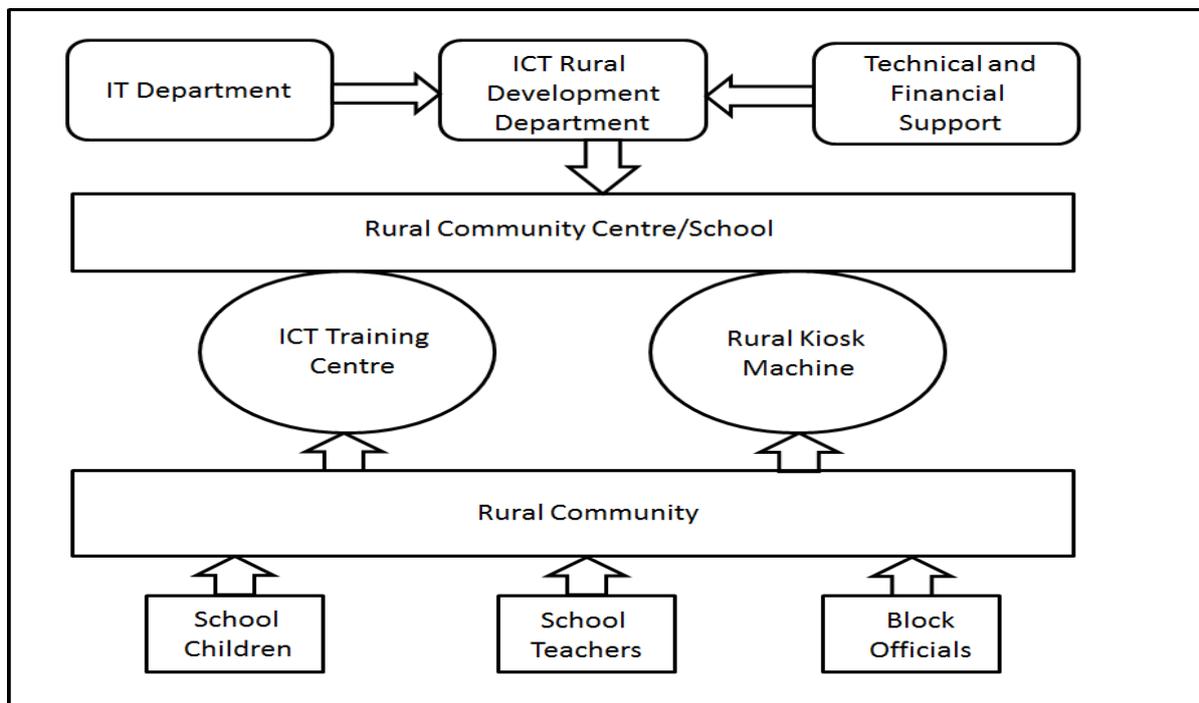
At the Entry level of the above framework, the Department of Education (2007) states that educators should acquire the basic skills and knowledge of ICT. At the Adoption and Adaptation levels, educators should acquire the integrative ICT knowledge and skills; and at the Appropriation and Innovation levels of the framework, they should acquire the specialised ICT knowledge and skills. This framework serves as a guide for educators to gauge the levels of ICT skills and knowledge they need to acquire in order to effectively use ICT in education.

The building block that was identified from this framework is *innovation*, and it will also be used in the formulation of the framework proposed in this research. According to the literature review conducted, innovation is one of the key elements for integrating ICT into the South African education system. New and innovative ways of using technology (ICT) should be used to enhance and integrate ICT security awareness into the South African

education system. The Teacher Development Framework is important because it is aimed at teachers, and teachers are responsible for the education of school learners.

### 4.3.3 Model for ICT Rural Education

The Model for ICT Rural Education is used to assist with the integration of ICT in rural schools in India (Roy, 2012). In this model Roy (2012) proposes numerous interactions between different stakeholders who have an interest in the development of rural areas in India. The Model for ICT Rural Education is depicted in Figure 4.6.



**Figure 4.6: Model for ICT Rural Education (Roy 2012)**

Even though the model looks as if it could be ideal for South African schools, it seems to require large financial support (for the establishment and maintenance of the ICT infrastructure). If it were to be implemented in South Africa, it would also require support from the rural communities involved.

One of the main components of the model for ICT Rural Education is school children, and they are also the main focus of the research in hand. Some of the other building blocks from this model are ICT training centre, community and technical and financial support.

## 4.4 Conclusion

This chapter presented the models and frameworks for ICT security awareness and ICT in Education and both spheres were discussed thoroughly.

The three models depicted in Section 4.3 were used to identify the building blocks for the framework to be proposed in this research. In each model or framework, one or more building blocks were identified that will be used to construct the proposed framework.

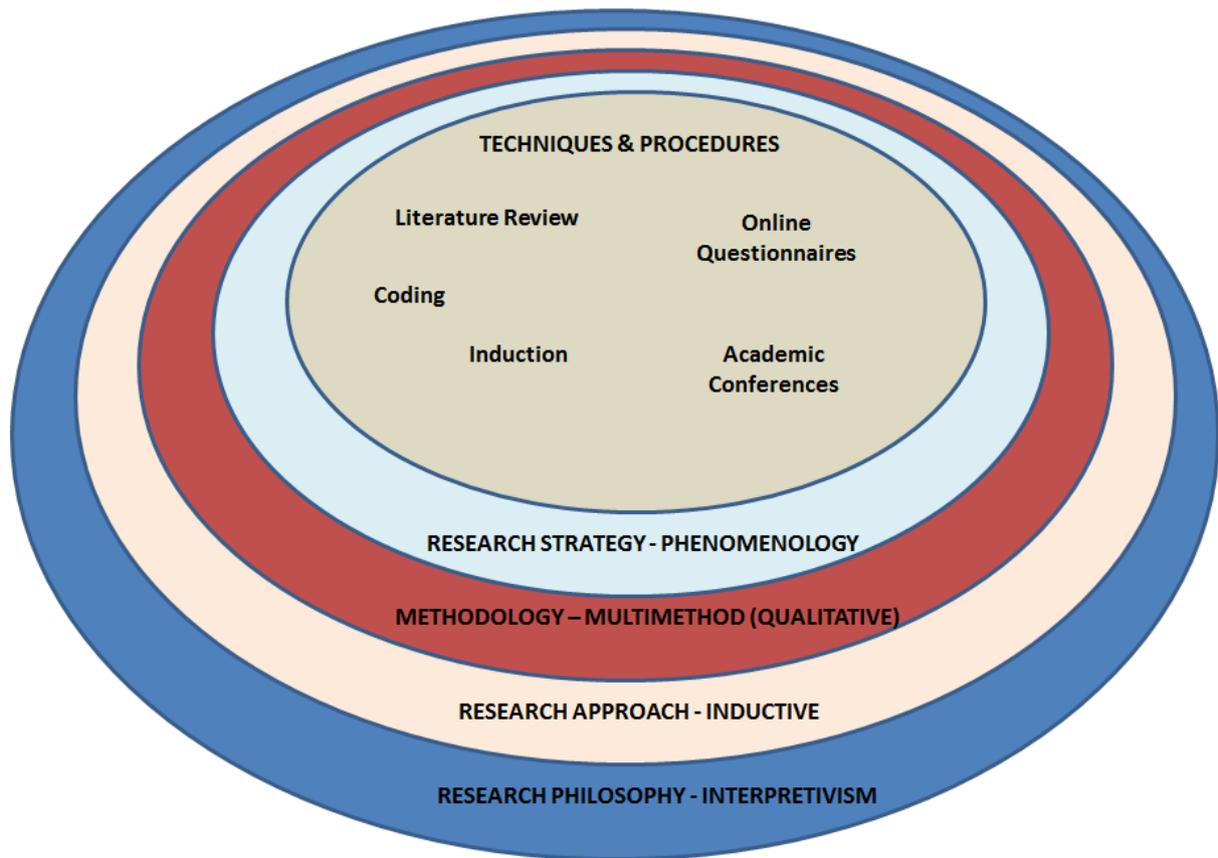
# Chapter 5: Research Methodology

## 5.1 Introduction

This chapter describes the research design that was applied in this research. It focuses on a discussion of the research philosophy chosen, the research approach, the methodology, the research strategy, and lastly the techniques and procedures that were used in the current research. Figures 5.1 and 5.2 attempt to clarify the research process by using diagrams, but in most of this chapter plain text explanation is done.

## 5.2 Research Design

The research design that is implemented in this research is based on the top-down research onion approach as implemented by Swanepoel (2015) and originally developed by Saunders et al. (2012). This approach is depicted in Figure 5.1 and it presents an outline of the research, as well as the reasons for selecting the particular components in the subsections that follow.



**Figure 5.1: Research Outline (based on Swanepoel 2015)**

The top-down approach and research outline depicted in Figure 5.1 is discussed in the subsections that follow. It starts from the outer part of the ‘onion’ (research philosophy) down to the innermost part (techniques and procedures).

### 5.2.1 Research Philosophy – Interpretivism

According to Saunders et. al (2008), interpretivism is a way that humans attempt to make sense of the world. It is a research philosophy that involves the interpretation elements of the study and it integrates human interest in that particular study. Interpretivism involves understanding the meaning of life. The attempts to understand the usage of ICT in South African education as well the integration of ICT security awareness into the system justifies the choice for this philosophy. In this study, the researcher interprets the factors that cause the non-integration of ICT security awareness into the South African education system by using the interpretivist research philosophy.

Based on an in-depth literature review, the researcher determined that there is a lack of ICT security awareness among school learners in South Africa and a notable gap between the two spheres of ICT security awareness and ICT in education. To bridge this gap and solve the problem of a lack of ICT security awareness among South African school learners, a framework that would attempt to resolve (or at least alleviate) these issues was proposed. This required the identification and interpretation of the trends from current literature and also the identification of those trends that can assist in solving the problem. Therefore, an interpretivist research design was seen as the suitable research philosophy for this research. According to Olivier (2004), the goal of interpretive research is to understand that which is being studied. Interpretivism was therefore used to understand the state of ICT security awareness among South African school learners, as well as to identify the gap that exists between the two spheres of ICT security awareness and ICT in education.

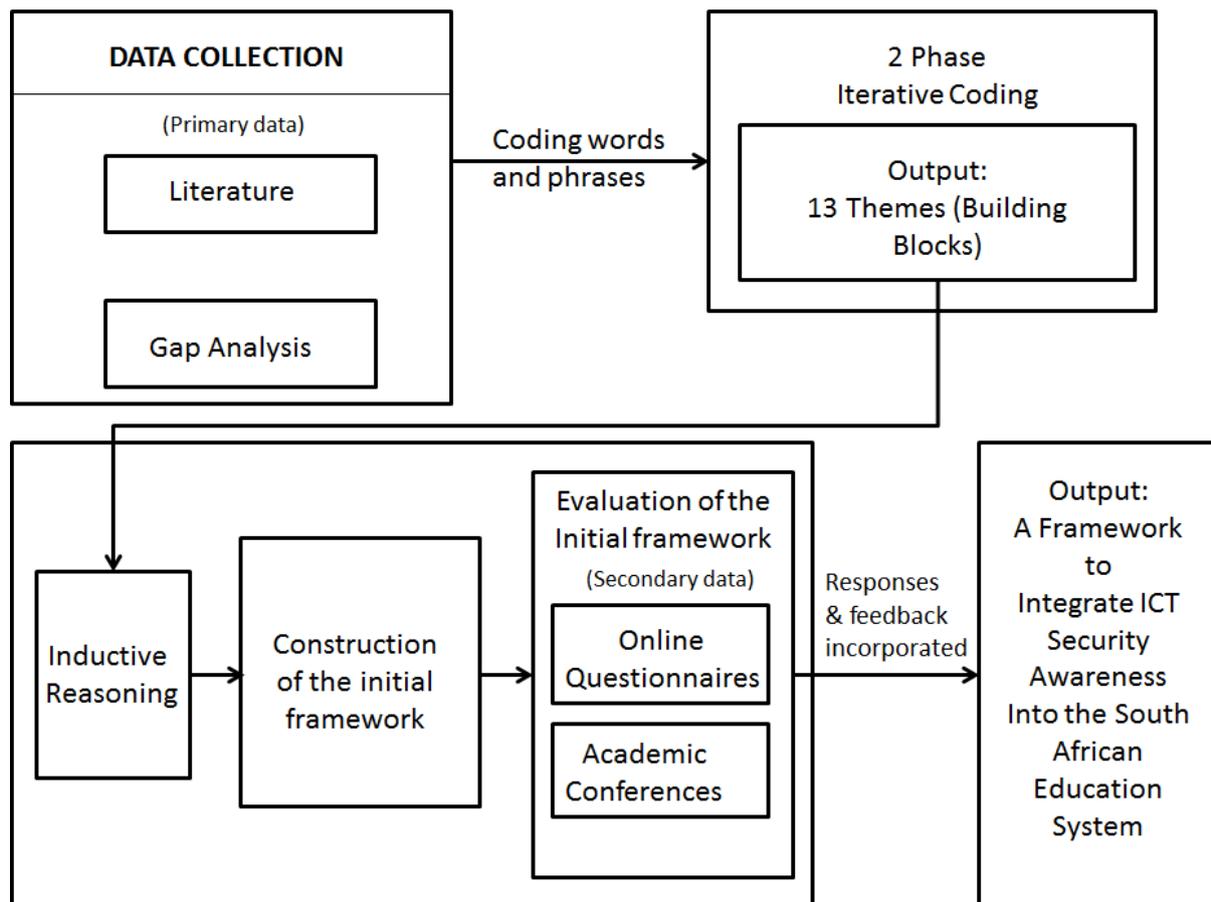
### 5.2.2 Research Approach – Inductive Approach

The literature review that was conducted in this research found no suitable framework that addresses the gap between the two spheres of ICT security awareness and ICT in education in South Africa. Therefore, an inductive approach (Creswell, 2009) was used to formulate and construct a framework that can assist with integrating ICT security awareness into the South African education system.

By using the inductive approach, the essence of the research objectives can be identified from the raw data (Creswell, 2009). This means that the raw data is summarised into codes and themes (building blocks), after which an analysis of the identified codes is conducted with the view of matching them with the research objectives. Lastly, a framework related to the research objectives of the research and the raw data acquired from the literature review needs to be developed (Swanepoel, 2015).

The data for constructing the framework proposed in this research was acquired from the literature, following a gap analysis. The potential use of the framework was evaluated through online questionnaires and peer-reviewed academic conferences. The online questionnaires and the academic conferences served as focus groups and were used to collect secondary data for indicating the potential usefulness of the proposed framework. The data that was acquired from the online questionnaires and academic conferences was

interpreted to make a preliminary evaluation of the framework that can be used to integrate ICT security awareness into the South African education system. Figure 5.2 depicts the research process that is aligned to the inductive approach that was used in this research.



**Figure 5.2: Inductive analysis process** (adopted from Swanepoel 2015)

Primary data was acquired from the available literature and the gap analysis table, while secondary data was obtained from the online questionnaires and academic conferences. The data was analysed using codes and themes to determine the themes (building blocks) that would be suitable for inclusion in the proposed framework. The output of the coding process produced 13 themes that were used for the formulation and construction of the framework.

### 5.2.3 Methodological Choice – Multimethod Qualitative Study

A multimethod qualitative study was the methodological choice used in this research. The data collection and analysis was done qualitatively (see Section 5.2.5 – Data Analysis – Inductive Analysis). To collect data, the researcher made use of an extensive literature review, the gap analysis table, and focus groups, which comprised of online questionnaires respondents and the academic conferences.

The process of inductive data analysis led to the coding of the literature through identification, interpretation, and the consolidation of the codes into 24 categories, which were further reduced to 13 themes (building blocks). A gap analysis table used the identified themes to determine the gap between the two spheres of ICT security awareness and ICT in education. These themes or building blocks were used as the basis for the formulation and construction of a framework that can be used to integrate ICT security awareness into the South African education system.

### 5.2.4 Research Strategy – Phenomenology

Phenomenology is a research strategy that focuses on the study of consciousness and a result of direct experience as described by the research participants (Creswell, 2009). This research is therefore regarded as a phenomenological study because firstly it has been presented at three different peer-reviewed academic conferences, and secondly an online questionnaire was sent to research participants to review it. On both the conferences and the online questionnaires, positive feedback was received and it was subsequently incorporated back to the research in order to improve it.

The use of phenomenology in this research assisted in understanding the phenomenon of ICT security awareness in South African education, the situation wherein this phenomenon is placed, as well as the perceptions of the experts who participated in the research (Creswell, 2009). The experts who participated in the evaluation have many years of experience – both in the ICT security industry and in academia in South Africa.

The experiences and perceptions of experts in the fields of ICT security awareness and ICT in education in respect of the framework were investigated, and this resulted in output that

was narrative as opposed to numerical. According to Swanepoel (2015), the narrative data is of a qualitative nature and therefore requires qualitative methods for its acquisition and analysis. This is the reason why a qualitative data analysis was used to investigate ICT security awareness in the South African education system.

### 5.2.5 Techniques and Procedures

The data collection methods and techniques that were used in this research were based on the type of data that was at disposal during the literature review. The literature review yielded qualitative data to be collected and analysed.

#### Data Collection Techniques

##### Literature review

An in-depth literature review was conducted to gather information about ICT security awareness in the South African education system. According to Olivier (2004), a literature review provides the researcher with related research topics, research approaches and research methodologies. It also assists the researcher in gaining knowledge and a better understanding of the research topic. A good literature review will show the researcher where his/her work fits into the existing body of knowledge. A thorough review of the literature was made in this research to ensure that the existing body of knowledge was covered.

##### Online Questionnaires (Focus Group 1)

The online questionnaire was used as a data collection technique in the pilot study of this research. According to Romm and Phil (2013), a questionnaire is a research method that is used to measure and analyse relationships between identified variables that exist in social reality. The aim of this online questionnaire was to obtain the views and opinions of participants regarding the proposed framework. Its purpose was to determine whether the participants considered the framework to be relevant to the South African context and to get their opinion on whether any other building blocks could be added to the proposed framework.

Open-ended interview questions were used in this research and the online questionnaires were sent to experts in their respective fields. According to Olivier (2004), surveys are conducted by sending questionnaires to a number of people to complete or by obtaining the answers through interviewing participants. The online questionnaires were sent to experts in the fields of ICT security awareness and ICT in education with a view to getting their views and opinions regarding the proposed framework. Feedback and responses were received in respect of the online questionnaires and some of the feedback that was received was incorporated into the proposed framework (SAISAFE).

Oates (2011) emphasises the importance of a well-designed and precise questionnaire. This increases the response rate and encourages the participants to continue and complete the questionnaire. The online questionnaire that was sent to participants in this research was well-designed and precise. No complaints were received from the participants about the quality of the online questionnaire. Oates (2011) adds that the questions in the questionnaire must be brief, relevant, unambiguous, specific, and objective. The online questionnaire that was used in this research contained open-ended questions, which made comments possible and facilitated the interpretation of the qualitative data.

As stated above, the online questionnaire was sent out to academia and industry experts to get their views and opinions on the proposed framework. The questions that were included in the questionnaire were such that all the necessary information could be gathered from the responses received from the experts. Experts from both the field of ICT security awareness and ICT in education were requested to complete the online questionnaire. The questions included in the online questionnaire gauged the effectiveness of the proposed framework. The questionnaire comprised of only one section that contained 19 questions. The information (responses and feedback) that was gathered by means of the online questionnaire is discussed and analysed in Chapter 8 of this dissertation.

### **The Selection of Participants**

Participants were selected by contacting both industry and academic experts in the field of ICT security awareness and ICT in education. Fifteen questionnaires were sent to individuals who were deemed experts in their respective domains. The eight experts who were eventually used as research participants in this research boasted many years of experience

in the ICT-in-Education and the ICT Security Awareness domains. Many of them had both academic and industry experience, which put them in a better position to comment and provide feedback, and it also granted them the unofficial authority to criticise constructively.

The credibility of the experts was considered by scrutinising their work experience, their qualifications, and their number of years working in the ICT Security Awareness and ICT-in-Education domains. Participant 1 reported having been in the ICT industry since 1973 and had wide experience in e-education. Participant 2 had obtained a number of qualifications and authored numerous publications. Participant 3 worked as a consultant for the Department of Basic Education (DBE) and had founded an NGO. Participants 5 and 6 were working in projects related to this research (such as ICT4D) and had many years' experience in the ICT industry. Participants 7 and 8 were also respectable academics with many years' experience in the topic of this research.

### **The Collection of the Data**

Primary data was collected through the use of an in-depth process of literature review. A gap analysis table that had been made up of themes (building blocks) coded from the literature review was also used as a form of collection of primary data. Secondary data was collected from the responses received from online questionnaires and academic conferences. The responses received from these secondary data sources were incorporated into the final version of the framework.

### **Peer-reviewed Academic Conferences (Focus Group 2)**

Three academic research articles were written, published and presented by the researcher at different peer-reviewed academic conferences in South Africa, namely SAICSIT2014, InfoSec2015, and ISTE2015. The conferences were used as focus groups to gain experts' perspectives and insight on the proposed framework and the situation of ICT security awareness in South African education.

Very informative and constructive responses were received from all these audiences. During the Saicsit2014 conference, the audience acknowledged the relevance of the proposed framework but also suggested that there was a need to expand it and make it more relevant

to South Africa. They also suggested the addition of more building blocks that would give the proposed more depth. The comments and feedback from the audience were noted and an effort was made to incorporate them into a newer version of the proposed framework.

A much improved and refined proposed framework was presented during the InfoSec2015 academic conference in Cape Town. Academics and experts in ICT security also acknowledged the relevance of the framework and suggested a number of improvements. The suggestions and improvements that were raised included the importance of structuring the framework properly so that it reflects the target. This resulted in the addition of the high school and primary school blocks in the proposed framework.

When the framework was presented at the ISTE2015, a lot of improvement emanating from the feedback received from the other conferences had been incorporated. The audience, which was mostly from the South African education system background, acknowledged the framework. They indicated that they were eager to see its implementation in the South African education system. All in all the feedback and responses received at the conferences assisted a great deal in constructing the final version of the proposed framework.

## Data Analysis – Inductive Analysis

The data that was received from the online questionnaires and the literature review was analysed by inductive reasoning. Swanepoel (2015) states that the inductive approach involves the construction of a framework that reflects a research objective from raw data collected during research. Inductive analysis is the process of identifying concepts from raw data and using those concepts to construct a theory or framework that describes a research topic through a process of inductive reasoning. This constitutes the analysis that was conducted in this research.

### **The Coding Process**

Data from the online questionnaires was used as input for Phase 1 of the coding process. In this phase the words, phrases and text were coded literally without trying to understand the meaning beyond the text. The codes that were acquired served as part of the building blocks that were used to construct the proposed framework. The output of Phase 1 was then used by re-coding the responses received from the online questionnaires. Phase 2

therefore interpreted the output received from Phase 1 by analysing the responses received from the online questionnaires and the literature review, and by eliminating all the repetitions and similar codes. The output of Phase 2 was 13 themes (building blocks) that could be used to construct the proposed framework. The themes were subsequently arranged to formulate and construct a flowing and understandable framework that attempts to resolve the problem of the lack of ICT security awareness in the South African education system.

### **Development of the Themes**

The codes that appeared more frequently in the online questionnaire responses and the literature review were used. Themes were chosen after scrutinising the responses and literature, and the researcher specifically looked for:

- The suggestions made by the online questionnaire respondents
- The frequency of the codes in the literature and online questionnaire responses
- The prevalence of the codes in the online questionnaire responses and conference feedback

The development and selection of themes ensured that the proposed framework would be relevant and would be aligned to the research objectives stated in this research.

### **Using the Themes to formulate a Framework**

An initial framework was formulated by means of generalisation and the comparison of themes with codes from the available data (online questionnaires, literature review, and gap analysis). Focus groups in the form of peer-reviewed academic conferences were also used to determine the viability of the framework in the South African context.

## **5.2.6 Verification – Proof of Concept**

For verification, peer-reviewed academic conferences were used to present research articles about the proposed framework. The data that was received from the conferences and the responses from the online questionnaires were analysed and incorporated into the final version of the proposed framework. Even though a fully-fledged proof of concept was not

done, the responses received from the online questionnaires showed that the framework had the potential to be useful.

## 5.3 Conclusion

Chapter 5 discussed the research approach that was used to formulate and propose a framework for the integration of ICT security awareness into the South African education system. It described the different components of the research methodologies used and provided justification for choosing specific research methodologies through the use of the 'research onion'.

# Chapter 6: The Design of the SAISAFE

## 6.1 Introduction

This chapter explains the process that was used to identify the gaps in the models and frameworks that were studied in this research. Some of these models and frameworks were used in the framework analysis (see Table 5.1) of this research.

An analysis of the various models and frameworks (the Comprehensive Information Security Framework (Da Veiga, 2008); the Business Model for Information Security (ISACA, 2009); the Information Security Retrieval and Awareness model (Kritzinger, 2006); the Four In Balance Model (Draper, 2010); the Teacher Development Framework (Department of Education 2007; Ndlovu & Lawrence 2012); and the Model for ICT Rural Education (Roy, 2012)) was conducted. The analysis presented an opportunity to propose a framework to integrate ICT security awareness into the South African schooling environment (Walaza, Looek and Kritzinger, 2014). Even though the current research focuses mainly on ICT security awareness in South African education, six models and frameworks from studies conducted in other countries were analysed.

ICT security awareness studies are not limited to the ones that were used in the table showing the analysis of models and frameworks. Various studies have been conducted in many different countries around the world. For instance, Saleh, Heba and Mashhour (2011) proposed a framework for security risk assessment and provided analysis that assisted in identifying system threats and vulnerabilities. Alnatheer and Nelson (2009) conducted research about the information security culture in Saudi Arabia and proposed a framework that could be used to identify and investigate factors that would assist in the implementation and adoption of an information security culture in that country. Thus, in addition to the models and frameworks that were used in this research, similar ICT security awareness studies were also conducted in other countries – which shows that ICT security awareness concerns exist not only in South Africa, but also in other countries. The scope of the problem is worldwide.

The models and frameworks mentioned in the paragraph above could not be used because of the topic and angle of the current research study. The study focused on ICT security awareness and ICT-in-education models and frameworks; and the chosen frameworks had

to be relevant to South Africa to some degree. Guided by the extensive literature review that was conducted and the criteria mentioned above, six models and frameworks were chosen. The analysis of models and frameworks is depicted in Table 6.1, while the results of the gap analysis are shown in Figure 6.1. A discussion of the table showing the analysis of models and frameworks, and of the figure showing the results also follow in this chapter. Section 6.2 next explains the analysis of models and frameworks.

## 6.2 Analysis of Models and Frameworks

This section presents a table to depict the gap that was identified after studying the various models and frameworks mentioned in Section 4. Walaza et al. (2014) analysed the models and frameworks in table format to illustrate what components are missing when it comes to ICT security awareness in South African education. Table 6.1 depicts the analysis based on a comparison of the ICT security awareness models and frameworks with ICT models and frameworks in education. Different building blocks were identified from various models and frameworks as they could be relevant to the proposed framework and make it more suitable for the South African context.

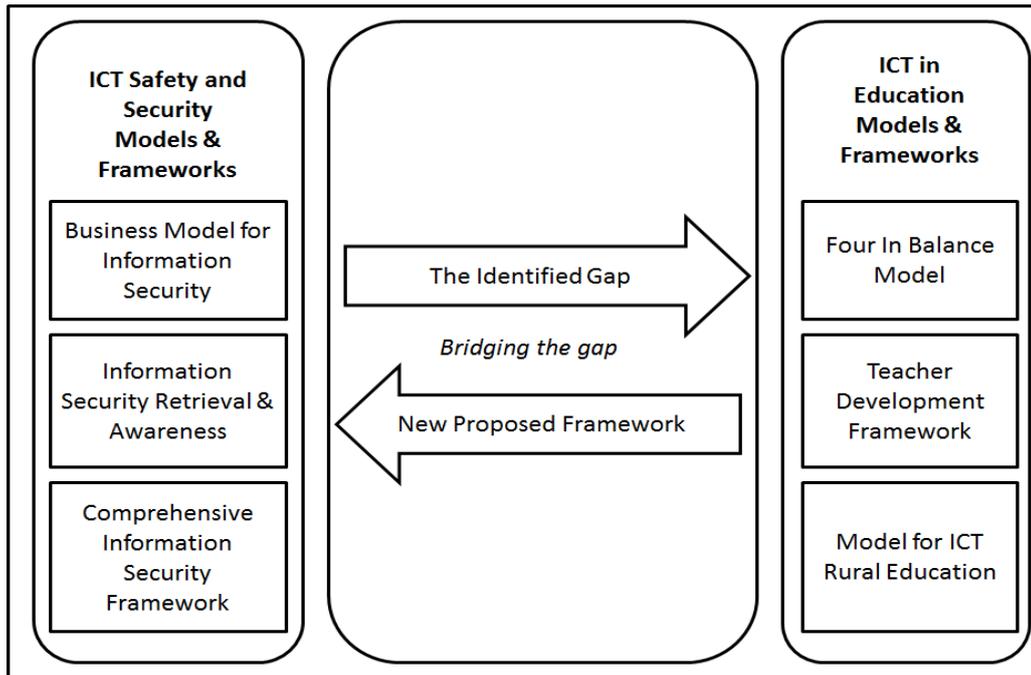
**Table 6.1: The Analysis of Models and Frameworks**

	<b>A - The Information Security Retrieval and Awareness (ISRA) model (Kritzinger, 2006)</b>	<b>B - The Business Model for Information Security (ISACA, 2009)</b>	<b>C - The Comprehensive Information Security Framework (CISF) (Da Veiga, 2008)</b>	<b>D - The Teacher Development Framework (Department of Education, 2007)</b>	<b>E - The Four In Balance Model (Drapeer, 2010)</b>	<b>F - The Model for ICT Rural Education (Roy, 2012)</b>
<b>Leadership and governance</b>		<b>X</b>	<b>X</b>		<b>X</b>	
<b>User awareness</b>	<b>X</b>		<b>X</b>			
<b>Information security documentation</b>	<b>X</b>		<b>X</b>			
<b>Policies and standards</b>			<b>X</b>			
<b>Code of best practice</b>			<b>X</b>			
<b>Human factors</b>		<b>X</b>				<b>X</b>
<b>Collaboration and support</b>		<b>X</b>			<b>X</b>	<b>X</b>
<b>ICT training and learning centres</b>			<b>X</b>			<b>X</b>
<b>Measuring and monitoring</b>	<b>X</b>		<b>X</b>			
<b>Innovation and technology</b>		<b>X</b>		<b>X</b>		
<b>Incident management</b>	<b>X</b>		<b>X</b>			
<b>Compliance</b>			<b>X</b>			
<b>School children</b>		<b>X</b>				<b>X</b>

Table 6.1 reflects the building blocks that were identified by Walaza et al. (2014) – written in bold – in the left-most column of the table. The different models and frameworks from which the building blocks were derived are listed in bold in the first row and marked as A, B, C, D, E, and F. The letter “X” is used to identify the building blocks that were found in more than one model or framework. Table 6.1 reflects involvement higher number of Xs on the ICT security awareness models and frameworks than on the ICT in education models and frameworks. This observation led to the conclusion that there is a gap between the two spheres. Hence, a comprehensive framework to integrate ICT security awareness into the South African schooling system is proposed.

### 6.3 The Analysis of Models and Frameworks Results

As is evident from Table 6.1, there is a notable gap between the ICT security awareness models and frameworks and the ICT-in-education models and frameworks. The ICT security awareness models and frameworks currently do not include ICT in education. Therefore, the framework that is proposed in this research will integrate the ICT security awareness models and frameworks with the ICT-in-education models and frameworks. Figure 6.1 depicts the current situation formulated on the basis of the analysis reported on in Table 6.1.



**Figure 6.1: Results of the Analysis of Models and Frameworks**

Figure 6.1 shows the results that were formulated from the analysis of models and frameworks in Table 6.1. The aim of the framework proposed in this research was to bridge the gap depicted in Figure 6.1 and to integrate the ICT security awareness with the ICT-in-education models and frameworks. The intention was to formulate a framework that would be inclusive of both sides and one that is relevant to the South African context.

## 6.4 Conclusion

This chapter presented an overview and analysis of the models-and-frameworks table (Table 6.1) that was formulated by using the building blocks derived from various ICT models and frameworks. The table depicts the derived building blocks (rows) as well as the models and frameworks (columns) from which they were derived. The results of the analysis of models and frameworks were also presented in Figure 6.1.

This chapter also depicted the gap that exists between the two spheres, namely ICT-in-Education models and frameworks and the ICT security awareness models and frameworks. The various building blocks that were used for the construction of the proposed framework will next be discussed in Chapter 7.

# Chapter 7: Discussion of the building blocks

## 7.1 Introduction

The main aim of this research is to propose a framework that will assist with the integration of ICT security awareness into the South African schooling system. Having discussed the various models and frameworks in Chapter 4, the research methodology in Chapter 5, and the design of the proposed framework in Chapter 6, the building blocks that were used for the construction of the SAISAFE are now discussed in this chapter. An overview of the building blocks is given in Section 7.2, followed by a discussion of each building block that was used.

## 7.2 The Building Blocks – Overview

This section presents the different building blocks that were used in the proposed framework and gives a brief introduction and overview of each. The building blocks were selected based on an in-depth literature review and analysis, as the researcher thoroughly studied the literature and encountered a number of frameworks and models related to the subject. He subsequently used the technique of identifying themes to determine the building blocks that would be used in this research. Jabareen (2009) mentions two methods of building a framework, namely: the grouping and labelling of similar data, and the identification of the connection between concepts by means of their relationship. This is precisely the method that was used in this research to identify the building blocks.

The proposed framework was named the South African ICT Security Awareness Framework for Education (SAISAFE). It comprises five main components: Leadership & Governance; Documentation; Collaboration & Support; People; and User Awareness. Within these components are sub-components that will be depicted and discussed briefly in Sections 7.2.1 to 7.2.13.

### 7.2.1 Leadership and Governance

The *leadership and governance* building block was chosen to emphasise the importance of involving and including the South African government in this initiative. Leadership and governance will be required from the South African government in order to integrate ICT

security awareness into the South African education system. Without the intervention and the involvement of the Department of Education and all related ICT security stakeholders, this integration will not be possible.

It is imperative for the South African government to play an effective leadership role in ICT security awareness in the country. ICT security governance is critical for any organisation, and it can serve as a catalyst for effective management and monitoring of information assets (Edwards, 2013). The South African government, by virtue of being the main custodian of education in the country, should play an effective leadership and governance role in the integration of ICT security awareness in the South African education system.

The Department of Telecommunications and Postal Services (DTPS), the Department of Science and Technology (DST), the Department of Communications (DoC), and the Independent Communications Authority of South Africa (ICASA) are the main custodians of ICT on behalf of the South African government. The responsibility for ICT in South African education lies with the Department of Basic Education (DBE) and the Department of Higher Education and Training (DHET). Therefore, it is their responsibility to ensure an accepted level of ICT security awareness among school learners. These institutions need to play a more vocal and visual role in improving and enhancing the level of ICT security awareness in the country.

It is also in these institutions' best interest to ensure that there is sufficient ICT security awareness among South African citizens. They must play a leadership role in ensuring ICT security and ensure that there is ICT awareness among South African citizens, especially the young people of South Africa. These institutions must delegate or govern the usage of ICT in the country and they need to come up with ways to ensure a sufficient level of ICT security awareness.

### 7.2.2 User Awareness

The *user awareness* building block was chosen because it represents the main subject of the current research. It was imperative to add this building block in the formulation of the proposed framework as the research aims to integrate ICT security awareness into the South African education system. This building block represents all the ICT security

awareness initiatives and programmes that are recommended and presented in this research.

The increased usage of ICT by young children has both advantages and disadvantages (Von Solms and Von Solms, 2014). Some of the major disadvantages of young children's use of computers (with access to the internet) are issues such as musculoskeletal disorders, exposure to pornography, and cyber-bullying (Kritzinger and Padayachee, 2007). It is for these and other reasons that Straker et al. (2010) stress the importance of teaching children about the wise usage of computers. This section investigates the user awareness component of the SAISAFE.

With South African school learners being among the top users of technology in the country (MyBroadband, 2014), it is imperative that they are equipped with as much ICT security awareness and knowledge as possible. Von Solms and Von Solms (2014) state that it is important for young children to be made aware of the dangers of the cyber-space already while they are young. The increase of cyber-crime in the country and reports published in the media (MyBroadband, 2014) have shown that there is a need for increased ICT security awareness among young people in the country.

One of the important aspects that should be looked at during the process of teaching school learners about ICT security awareness is changing their attitudes and behaviour. Knowledge alone is not enough for people to act differently; their mind-sets and behaviour need to be changed as well (Gundu and Flowerday, 2013). This research proposes rigorous repetitive ICT security awareness initiatives directed towards school learners. This will help to ensure that school learners are constantly reminded about the dangers of ICT and technology in general.

The cyber-crimes that occurred in recent years in South Africa mostly took place in banking institutions and sadly these institutions have refused to take responsibility for these crimes (Belayneh, no date). Given the vulnerabilities of children in South Africa and the level of crime in the country, it is of utmost importance that school learners are made aware of ICT security. Especially children in the rural areas often face risks such as human trafficking, rape and cyber-bullying. It is, therefore, important to ensure that the level of security awareness among school learners is high.

The education system can play a pivotal role in increasing ICT security awareness among young people (Von Solms and Von Solms, 2014). This research re-emphasises this fact by proposing that ICT security awareness be included in the South African school curriculum. One of the challenges that have contributed to the lack of ICT security awareness in South African schools is that the teachers themselves are not adequately equipped to deal with ICT security. The integration of ICT security awareness into South African schools would first require school teachers to be trained about ICT security awareness. This would avail teachers the opportunity to gain knowledge and experience in this field.

### 7.2.3 Information Security Documentation

The literature review conducted as part of this study indicated a lack of sufficient ICT security documentation to assist with creating ICT security awareness in South Africa. The building block of *information security documentation* aims to emphasise the importance of raising ICT security awareness among South African school learners. Such documentation should be easily accessible to all South African school learners and to the public at large.

The Information Security Documentation building block was derived from the ISRA model. It provides all documentation necessary for information security and allows school learners to recognise ICT security awareness concerns and respond accordingly (The European Network and Information Security Agency (ENISA), 2010). The aim of this documentation is to enhance the knowledge and ICT security awareness of school learners in South Africa.

The South African government (as the main custodians of ICT in South Africa), private institutions like banks, and tertiary institutions need to create databases, libraries and information stores where ICT security awareness documentation can be kept and made available to all citizens of the country. According to the literature reviewed, these institutions are the ones that are mostly affected by ICT-related crime. Therefore, it will be in their best interest to ensure that their stakeholders (i.e. employees, customers, suppliers) and ordinary citizens who are able and willing to learn more about information security are forewarned.

Information security documentation should in particular be made available to all South African school learners. The more information security documentation is available, the

better the security awareness of everyone in the ICT industry and country at large. This research proposes that information security documentation should be made available at all public areas in South Africa. Places such as hospitals, churches, libraries, taxi ranks, etc. should be equipped with information kiosks that have information security documentation such as newsletters, pamphlets, research articles, and many more. It is also important that this content be made available to school learners at their respective schools.

#### 7.2.4 Policies and Standards

This building block, which was derived from the Comprehensive Information Security Framework (CISF), was chosen to emphasise and encourage the formulation of *policies and standards* that will govern the integration of ICT security awareness into the South African education system. It is imperative that the defined policies and standards are followed and adhered to during this integration process. This building block will also cater for the formulation of relevant standards and policies.

The policies and standards sub-component will look at the best policies and standards that must be adhered to by school learners in South Africa at all times. It will also aim to govern the usage of ICT by school learners in South Africa.

In South Africa it is the responsibility of government subsidiaries (like the Department of Communications and ICASA) to ensure that there are sufficient and effective policies and standards for ICT security awareness in place. These policies and standards can eliminate or at least reduce the ICT risks faced by school learners. Tertiary institutions can play a crucial role in assisting the government to formulate policies and standards that are relevant to South African school learners.

#### 7.2.5 Code of Best Practice

The *code of best practice* building block was also derived from the CISF and it was chosen to emphasise and propose a code of best practice that can be used for the integration of ICT security awareness into the South African education system. The purpose of this building block is to emphasise the importance of adhering to best practice during this process.

An effective code of best practice should be formulated for use by all South African school learners who make use of ICT. This code should be communicated to and enforced among all school learners in the country. It should also be explained to the learners that the code of best practice is implemented for their own benefit and for the betterment of the country (by fighting crime).

### 7.2.6 Human Factors

This building block was chosen to cater for all the *human factors* associated with the integration of ICT security awareness into the South African education system. All these factors will be gathered under this building block to be considered during the integration of ICT security awareness into the South African education system.

The *human factors* building block, which was derived from the Business Model for Information Security, will investigate some of the factors that might influence ICT security awareness among the South African school learners. These factors (whether challenges or benefits) will be identified and used for reference purposes when implementing ICT security awareness programmes in various schools in South Africa. They will also be considered when making decisions about the local curriculum for ICT security awareness. The human factors will also serve as basis for further research on ICT security awareness integration in South African schools.

Various factors contribute to the lack of ICT security awareness in South Africa, for instance culture, people's attitude towards technology, and even issues like ignorance. The human factor is a big issue when it comes to ICT security awareness in developing countries like South Africa. Factors such as low levels of education or inadequate education are a major problem in many developing countries.

### 7.2.7 Collaboration and Support

Based on the literature review, the researcher found that there is insufficient collaboration between and support from South African government institutions, academia, and the ICT private sector when it comes to ICT security awareness. The aim of this building block is to

propose and enhance *collaboration and support* among the stakeholders in the South African ICT security sector.

The Collaboration and Support building block was derived from the Four In Balance Model. In the current research, this component will be used to facilitate collaboration with regard to ICT security awareness among institutions in South Africa. Institutions such as universities and private companies will be requested to provide and disseminate ICT security awareness information among South African school learners. Private companies will also be requested to sponsor programmes to enhance ICT security awareness among South African school learners.

Tertiary institutions (e.g. the University of South Africa – UNISA), government institutions (e.g. the State Information Technology Agency – SITA), schools, and other stakeholders (e.g. Information Security South Africa – ISSA) need to collaborate to formulate support structures for teaching all school learners in South Africa about ICT security awareness and the dangers of ICT. Through such collaboration, ICT security awareness information can also be disseminated to learners in schools all over the country.

The South African government should furthermore set up a hotline to support victims of ICT-related crimes in South Africa. For instance, if someone encounters or falls victim to cyber-crime, they should be able to call a toll-free number where they will be assisted and advised on the necessary steps to take. The government should appoint an ombudsman to deal specifically with cyber-security complaints and victims of ICT-related crime in South Africa. This will assist in reducing the number of ICT-related crime incidents in the country.

### 7.2.8 ICT Learning and Training Centres

This building block, which was derived from the Model for ICT Rural Education model, was chosen to propose the founding of *ICT learning and training centres* in all strategic areas utilised by school learners in South Africa. It is not only in the classroom that school learners must be exposed to ICT security awareness – such exposure should be offered in as many places as possible.

This research suggests the construction of training and learning centres that will assist with ICT security awareness among all school learners. The centres will be built in convenient

places in both urban and rural areas around South Africa. The training centres will have books and computers that provide information about ICT security awareness. Schools and libraries can also be used to offer this functionality and to ensure that free and easy access to ICT security awareness information is provided to school learners in these centres.

The government of South Africa needs to set up adequate ICT training and learning centres around the country to educate school learners about ICT security awareness. One classroom in every school could be set up as a training and learning centre where school learners will be taught about ICT-related crime during their early schooling years.

### 7.2.9 Measuring and Monitoring

The *measuring and monitoring* building block, which was derived from the ISRA model, aims to measure and monitor the scope of initiatives for creating ICT security awareness among South African school learners. It will also determine the effectiveness and the impact of integrating ICT security awareness into the South African education system.

This building block will be used to measure and support ICT security awareness among school learners in South Africa by requesting support from the South African government. The Department of Education must ensure that ICT security awareness is established among the country's learners. The DOE must also ensure that appropriate mechanisms are in place to measure and monitor learners' usage of ICT and the level of their ICT security awareness. The gullibility of school learners makes it essential that their ICT usage be monitored and measured on an ongoing basis to ensure that they use ICT responsibly. Guidelines and rules should be written for all school learners who use ICT and they should be encouraged to abide by these instructions at all times.

Without compromising the privacy of school learners, it is of crucial importance that measuring and monitoring controls be put in place to overcome the problem of a lack of ICT security awareness in schools. The South African government needs to take responsibility for dealing with this situation and it should not only put measuring and monitoring controls in place, but ensure also that they are communicated to school learners across the country.

### 7.2.10 Innovation and Technology

This building block, which was derived from both the Teacher Development Framework and the Business Model for Information Security, was chosen to encourage the inclusion of *innovation and technology* when integrating ICT security awareness into South African education. With the advancement of technology in the world, the aim of this building block was to ensure that technology be utilised to its full extent during this process.

The building block proposes a number of innovative solutions and programmes to enhance and promote ICT security awareness among school learners. Technologies such as mobile phones, mobile apps and websites, as well innovations such as competitions, will be utilised to enhance and integrate ICT security awareness in South African schools and among school learners.

Stakeholders in ICT security awareness in South Africa need to come up with innovative ways of fighting ICT-related crime. It is evident that the perpetrators of ICT-related crimes in South Africa constantly find new ways of attacking their victims, which is why it is important to ensure that there are new ways to combat these crimes.

Government institutions (such as SITA) must organise more seminars like the Government Technology Conference (GovTech) and the Youth in Science, Innovation and Technology Indaba to get together ICT professionals, academics and experts from the ICT industry to come up with ideas to combat and assist in reducing ICT-related crimes in the country. The private sector can also play a role by sponsoring events and competitions where experts can be asked to devise new ways to try and combat these ICT-related crimes.

### 7.2.11 Incident Management

This building block, derived from the CISF framework, was chosen to ensure that *incident management* procedures are made available to all South African school learners. The literature review indicated that insufficient incident management procedures have been made available to victims of crime related to ICT security in South Africa. This building block will ensure that South African school learners are made aware of the procedures that must be followed when one has been a victim of ICT-related crime.

This component will also be responsible for documenting all incident management procedures that must be followed by school learners. The documentation will be distributed to school learners in South Africa and they will be trained or shown how to follow the procedures when needed.

The government of South Africa must ensure that there are sufficient incident management procedures in place to be used when ICT-related crimes occur. A trend that has been noticed over the past few years is that the local banks are continuously denying responsibility when ICT-related crimes occur; instead they are blaming their clients and citing negligence on the latter's side. An incident management plan will go a long way in assisting the victims of ICT-related crimes in South Africa.

### 7.2.12 Compliance

The *compliance* building block, also derived from the CISF, was chosen to promote agreement among all ICT stakeholders in South Africa. The integration of ICT security awareness into the South African education system must comply and be in line with the laws and policies that govern the usage of ICT in South Africa.

This component will investigate compliance among ICT stakeholders in South Africa, specifically among school learners. South Africa uses the ECT Act to govern the usage of ICT in the country. Policies such as the South African Cyber Security Policy have also been introduced in South Africa to try and reduce ICT-related crime (Department of Communications, 2010). This component aims to involve the South African government and all other ICT stakeholders to ensure that there is proper compliance with the ECT Act and with all other ICT security policies implemented in the country.

The custodians of ICT in South Africa must make sure that school learners comply with the laws of the country regarding ICT usage. It is also the government's responsibility to ensure that both school learners and all other institutions in the country obey and comply with the ECT Act.

### 7.2.13 School Learners

This building block, derived from the Model for ICT Rural Education model, was chosen to illustrate and re-emphasise *school learners* as the main focal point of this research. Local school learners will be the main beneficiaries of the integration of ICT security awareness into the South African education system; hence it is imperative that they are included as one of the building blocks for the formulation of the final proposed framework.

The researcher added two elements to the sub-component School Learners, called High School and Primary School, merely for the sake of making a distinction between the two types of school learners. According to Kortjan and Von Solms (2014) the content offered in education is dependent on the target audience. The ICT security awareness information and material that will be made available to school learners cannot be the same for all, because of the age differences between primary and secondary school learners.

A proposal is made in this research that ICT security awareness information and material be made available to the school learners in South Africa on a regular basis by making use of various types of media (mobile phones, television, websites, and so on). School learners must be kept abreast of the latest ICT security awareness information and material at all times, and this information must be available in a language that they understand. Caution must however be exercised and a clear distinction must be made by the relevant authorities on the type of information that is suitable for access by primary school learners as compared to high school learners.

School learners constitute one of the most important building blocks in this research, and the integration of ICT security awareness into the South African education system is the main focus of this research.

Certain other components also had to be added to make the proposed SAISAFE framework more relevant to the South African context (Walaza, Loock and Kritzing, 2014). These components are discussed thoroughly in Section 7.3.

## 7.3 An Overview of the Added Components

In the framework that was proposed by Walaza et al. (2014), it was alluded that certain extra components had to be introduced to ensure that the proposed framework is relevant to the South African schooling environment. This also implies that the framework could be adapted to include other components – in this case Language; ICT Security Ombudsman; ICT Security Curriculum, and Information Repositories. The added components are discussed briefly in Sections 7.3.1 to 7.3.4 and depicted in Figure 7.1.

### 7.3.1 Language

According to Ngcobo (2009), South Africa is widely commended for its policy of multilingualism, but the implementation of this policy remains a problem. The current research agrees and proposes that the dissemination of all information pertaining to ICT security awareness be done in the country's indigenous languages. Ngcobo (2009) also advises that modern strategies to assist with the implementation of the language policy should be adopted in South Africa – suggesting the first strategy as making information available in all official South African languages.

Many ICT-related software applications are developed with the incorrect assumption that it is easy for school learners to understand non-native languages (Roy *et al.*, 2014). South Africa has a diverse population and its eleven languages are used by school learners all over the country. Ngcobo (2009) suggests that the use of all official languages in South Africa should be accepted as a norm. UNESCO (2012) emphasises the importance of using native languages in learning by documenting that better results have been achieved when learners use their native languages. The points mentioned in the research done by Roy et al. (2014) and UNESCO (2012) indicate the importance of using native languages when dealing with ICT security awareness among school learners. The research makes it clear that it is easier to learn and understand if the language used is the learner's mother-tongue.

Even though this research recommends the usage of indigenous languages, the author is well-aware of the practical difficulties that this entails. School learners will have to be made aware of the importance of learning and knowing a universal language like English and not

limit themselves only to their home language. English is after all the software language used in most computer and mobile devices in South Africa. Isasig (2012) reiterates this view by mentioning the significance and importance of integrating a foreign language into teaching and learning. One of the benefits of knowing a world language is the user's exposure to the modern world and current global standards.

### 7.3.2 ICT Security Ombudsman

The office of the ICT security ombudsman is a concept proposed by this research, seeing that the literature review revealed the lack of such an office in South Africa. Since a number of ICT-related crimes occurred in recent years in the country (Belayneh, no date), having such an office would be beneficial to South Africa. Walaza et al. (2014) mention the high crime rate in South Africa and stress the need for proper ICT security awareness measures to be put in place. South Africa is seen to be lagging behind when it comes to ICT security awareness of its citizens (Department of Communications 2010; Kayle 2011). However, progress in the form of the development of a national cyber-security policy by the Department of Communications (2010; Francis 2010) has been seen in recent years.

Cyber-security is an important element in the attempt to bridge the digital divide in South Africa (Grobler, Vuuren and Leenen, 2012). In their research, Nevondwe and Odeku (2014) state that South Africa has become a haven for perpetrators of child pornography, even though the country is one of the top five countries in the world that has legislated meaningfully on it. This discrepancy re-emphasises the need for a body or an office that will be responsible and look after the interests of ICT security victims in South Africa.

The office of the South African ICT security ombudsman will perform duties similar to those of other ombudsman offices such as the insurance ombudsman, the tax ombudsman, and the banking ombudsman. In the event that a person has been a victim of ICT-related crime, would like to lay a complaint, or is struggling to get compensation from a service provider; then the victim will be able to contact this dedicated office. The office will conduct an investigation and pass judgement on the matter. The office of the ICT security ombudsman will require all the necessary support from the South African government and the private sector.

### 7.3.3 ICT Security Curriculum

Even though there have been attempts to equip schools and educators with the necessary ICT skills for (ICT related) curriculum delivery in South Africa, there is still evidence of low adoption of ICT among educators in schools (Chigona and Chigona, 2010). In their research, Kritzinger and Padayachee (2007) propose the inclusion of e-safety and ICT security awareness in the South African school curriculum. Ford and Botha (2010) also mourn the lack of integration of ICT into the local school curriculum. Hence, this research proposes that ICT security be included in the South African school curriculum.

De Lange and Von Solms (2013) argue that the school environment is the best place to make children aware of the dangers of the internet and teach them about ICT security awareness. It is imperative for children to be made aware of ICT security from a young age because nowadays they are exposed to the internet from an early age (De Lange and Von Solms, 2013). This makes children vulnerable to a number of internet dangers. The proposed curriculum will be specifically aimed at creating ICT-security awareness, and its purpose will be to enhance ICT security awareness among school learners in South Africa. Aloul (2012) suggests that schools and universities should run ICT security awareness campaigns and introduce ICT security awareness as a topic into their curriculum.

Research studies by Wayman and Kyobe (2012) and Kritzinger and Padayachee (2007) have shown that there is insufficient inclusion of ICT security awareness in the South African school curriculum. Wayman and Kyobe (2012) emphasise the importance of solving this problem and state that during their research (surveys and interviews), the participants showed a lack of knowledge of critical legislation such as the Protection of Personal Information (PoPI) Act, Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), and the Promotion of Access to Information Act (PAIA).

Content for this proposed curriculum has been sourced from reputable academic literature as well from relevant organisations that are interested in ICT security awareness in South Africa. Content depends on the audience to whom it is offered, for instance, some of it should be relevant for younger children, whereas the rest should be more relevant for older school learners (Kortjan and Von Solms, 2014). The ICT security curriculum should be kept

up to date and ensure that relevant standards are taught to the South African school learners.

### 7.3.4 Information Repositories

The research in hand proposes that the South African government (particularly the Department of Communications and the Department of Education) should set up information repositories that store information about ICT security awareness. These repositories will be used for information sharing and they must be easily and freely accessible to all school learners in South Africa. Learners at South African universities are continuously accessing and creating documents through online databases, emails, and research databases (Kyobe, Molai and Salie, 2009). The information in these repositories will consist of all the research related to ICT security awareness done in South Africa and around the world.

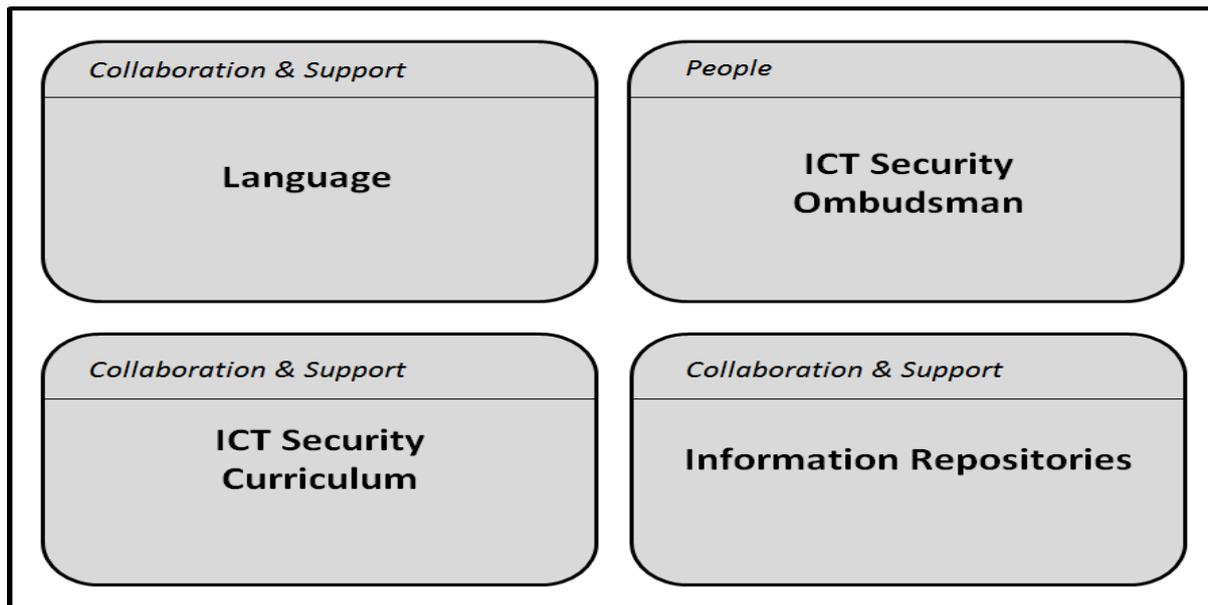
Due to factors such as lack of infrastructure and access to technology, the integration of ICT in education in developing countries has not been realised (Chigona & Chigona 2010; Roy 2012). Rotich and Munge (2007) state that online information-sharing networks have opened up new avenues of development in Kenya. These networks enable users to have access to a large amount of information. Information-sharing resources such as national and international databases have clearly played a major role in alleviating the scarcity of information in Kenyan schools (Rotich and Munge, 2007), and information repositories – a technique similar to the creation of online information-sharing networks – is proposed in this component.

The information repositories that have been proposed will be placed strategically in public areas where they can be easily accessible to everyone. They will serve as focal points where school learners (as well as ordinary citizens) can get all the information related to ICT security awareness that they might need, and they will take the form of mobile kiosks placed in appropriate areas such as police stations, libraries, hospitals, municipal offices and community halls. The information repositories will contain research papers related to ICT security awareness, websites, social networks, magazine articles, newspaper articles, and research articles in electronic and printed format.

The purpose of this added component is to increase the school learners' knowledge as well as their ICT security awareness.

### 7.3.5 Summary of the Added Components

Figure 7.1 depicts the components that have been added in order to make the proposed framework relevant to South Africa.



**Figure 7.1: The Added Components**

The top part of each component in Figure 7.1 is an indication of the phase in the proposed framework that the component belongs to. An overview of the proposed framework as well as the building blocks that were used are discussed in Section 7.4.

## 7.4 The South African ICT Security Awareness Framework for Education (SAISAFE)

The proposed framework is divided into five components: Leadership & Governance; Documentation; Collaboration & Support; People; and User Awareness.

The two main components of this framework (Leadership & Governance and User Awareness) communicate with the three remaining components (Documentation; Collaboration & Support; People). The Documentation and People components are inter-

linked with the Collaboration & Support component. Three of the components – Documentation, Collaboration & Support, and People – also contain sub-components.

The sections that follow provide an overview of the components and sub-components of the proposed framework.

### 7.4.1 Leadership and Governance

The *Leadership & Governance* component is a building block that was derived from the Comprehensive Information Security Framework (CISF) (Da Veiga, 2008). According to Da Veiga (2008) this component provides strategy and direction to the implementation of the CISF and will provide the same functionality in the proposed SAISAFE. The main custodians of ICT in South Africa (the South African government and the Department of Education) will have to play a leadership and governing role when it comes to the integration of ICT security awareness into South African education. The Leadership and Governance component refers to the custodians of ICT in South Africa and it is inter-connected with the three components that are in the middle (Documentation, Collaboration & Support, and People).

### 7.4.2 User Awareness

The *User Awareness* building block was also derived from the Comprehensive Information Security Framework (CISF), which according to Da Veiga (2008), can be used in different types of environments. The User Awareness component is responsible for ICT security awareness in this research, and programmes to ensure ICT security awareness among South African school children will be discussed extensively as part of this component. User awareness plays a critical role in this research and will include various sub-components to assist with the integration of the two spheres (ICT security awareness and ICT in Education).

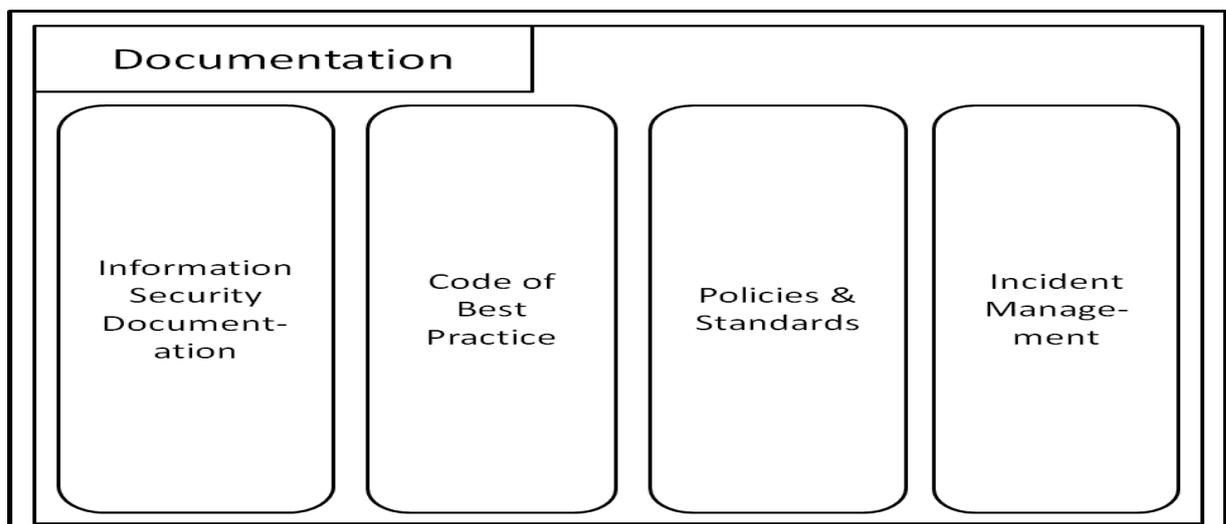
The User Awareness component refers to the ICT security awareness aspect of the SAISAFE and it is linked to three components of this framework, namely Documentation, Collaboration & Support, and People. It is important to all the components. User Awareness should be driven and enforced by the Leadership & Governance component, proper and effective documentation must be made available, collaboration and support structures must

be put in place, and all these resources must be made available to all ICT users (especially school learners).

### 7.4.3 Documentation

The Documentation component is a building block that was derived from the Information Security Retrieval and Awareness (ISRA) model (Kritzinger, 2006). Kritzinger (2006) states that the aim of the ISRA model is to enhance information security awareness among employees of an organisation. This building block will be used for all the documentation that is relevant to ICT security awareness in South African schools. Within this component are sub-components that depict the various ICT security awareness documents available in literature. They will be used to ensure the effective integration of the two spheres.

Figure 7.2 depicts the four sub-components within the Documentation component, namely Information Security Documentation; Code of Best Practice; Policies and Standards; and Incident Management. The purpose of this component is to record and document all relevant and important information relating to ICT security awareness and ICT education. This documentation will be used for the purposes of this research, to assist with the integration of ICT security awareness into the South African schooling system.

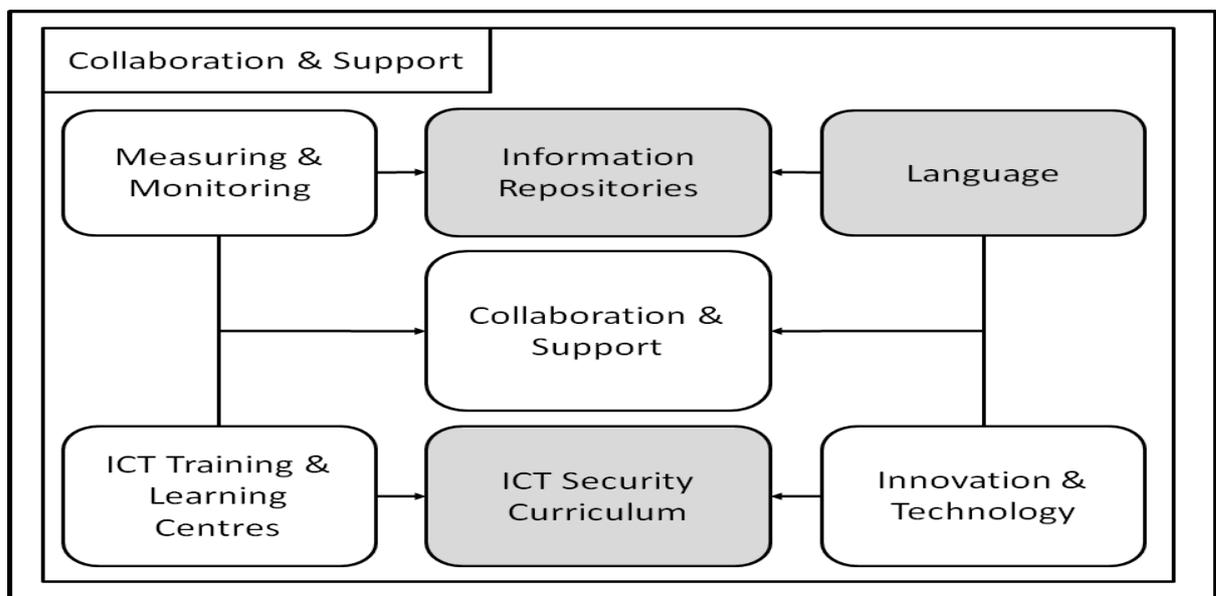


**Figure 7.2: The Documentation Component**

#### 7.4.4 Collaboration and Support

The Collaboration and Support component is a building block that was derived from the Four In Balance Model. Draper (2010) highlights teacher expertise as an important component of this model because teachers are the ones responsible for the safe usage of ICT in schools. In this research, the Collaboration & Support component will play the role of integrating the two spheres (ICT security awareness models and ICT-in-Education models) and it contains a number of sub-components that are used to ensure the integration of ICT security awareness into South African schools. Some of the additional sub-components introduced in this research will also be discussed within this component.

Figure 7.3 depicts the Collaboration & Support component of the proposed framework.



**Figure 7.3: The Collaboration and Support Component**

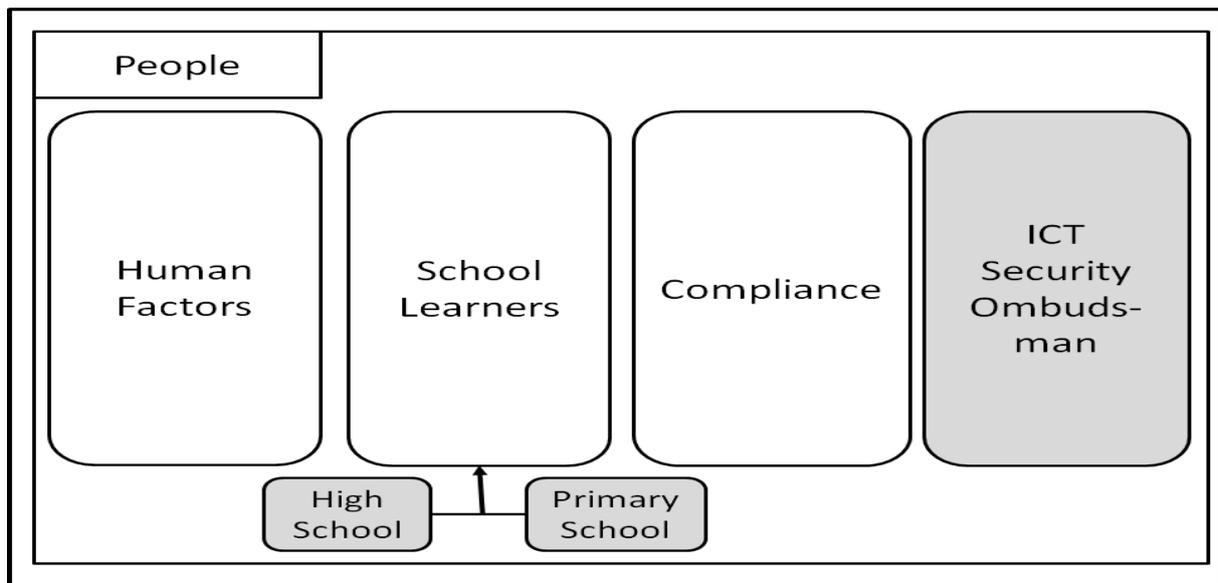
The four sub-components that are within the Collaboration & Support component are Measuring & Support, Collaboration & Support, ICT Training & Learning Centres, and Innovation & Technology. The current research also introduced three new components to make the proposed framework relevant to South Africa; these new components are Information Repositories, Language, and ICT Security Curriculum (see Section 5.3 of this research). The rest of the components are discussed in the upcoming paragraphs.

The Collaboration & Support component is located in the middle of this framework and consists of four sub-components, namely: Measuring & Monitoring, Collaboration & Support, ICT Training & Learning Centres, and Innovation & Technology. The sub-components within this component are linked together to show that each one is related to another and is just as important as the other. Collaboration & Support is the most important component of this framework because it connects all the other components with each other.

### 7.4.5 People

The People component is a building block that was derived from the Business Model for Information Security (ISACA, 2009) model. ISACA (2009) boasts that the ICASA model can be used in any type of organisation, hence it is also relevant for this research. The People component is responsible for all the human aspects in this research, and depicts and clearly defines the role played by each of them. The various human aspects will be depicted as sub-components within the people component. The proposed new sub-component, the ICT Security Ombudsman, will also be included.

Figure 7.4 depicts the People component of the proposed framework.

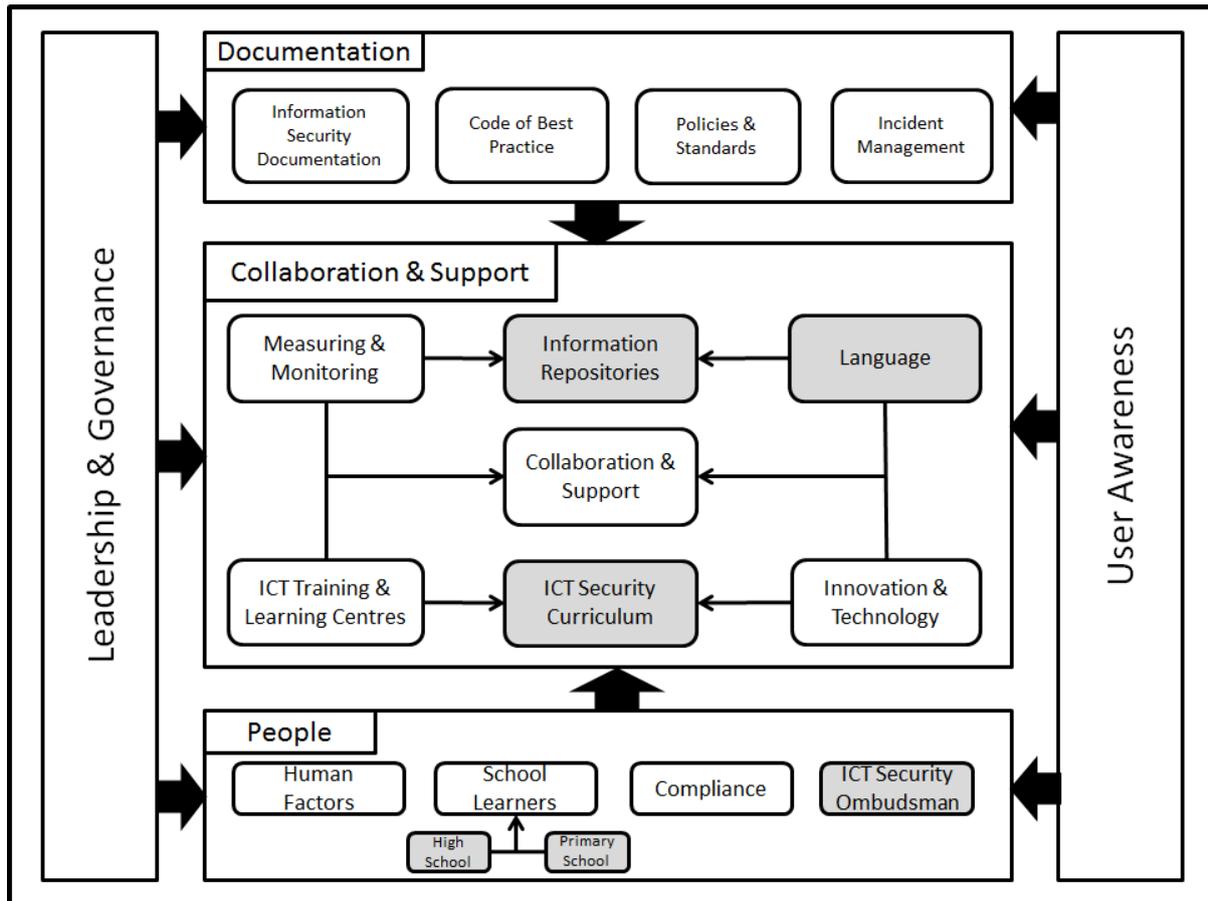


**Figure 7.4: The People Component**

The sub-components within the People component are Human Factors, School Learners and Compliance, as well as the new subcomponent, the ICT Security Ombudsman, which was introduced by the current research in order to make the proposed framework relevant to South Africa. The ICT security ombudsman was discussed among the other new subcomponents in Section 7.3. The School Learners subcomponent introduces two further elements called High School and Primary School. These and the rest of the subcomponents under the People component are discussed in the following paragraphs.

The People component consists of four sub-components, namely Human Factors, School Learners, Compliance, and ICT Security Ombudsman. This component is associated with the human aspect of this framework. All the sub-components within this component refer to human aspects of ICT security awareness in education. The People component is linked to the Collaboration & Support component as well as to the Leadership & Governance and User Awareness components.

Both the flow and the relationship between the various components of the SAISAFE are clearly depicted in Figure 7.5.



**Figure 7.5: South African ICT Security Awareness Framework for Education (SAISAFE)**

The components in the framework are all connected by means of arrows to indicate the dependability of the components on each other. The joining arrows indicate that no component exists on its own, and that all components work together to integrate ICT security awareness in South African schools. The newly proposed sub-components and elements are coloured in grey within the framework so as to distinguish the components that were derived as building blocks in Table 6.1 from existing models and frameworks.

The main purpose of the SAISAFE is the integration of ICT security awareness in South African education. The in-depth literature that was conducted in this research indicated that the existing models and frameworks were not relevant to South Africa. Hence a new framework relevant to South Africa – the SAISAFE – was proposed.

## 7.5 Conclusion

Chapter 7 explored the various components of the proposed framework, the South African ICT Security Awareness Framework for Education (SAISAFE) and depicted them in Figure 7.5. The SAISAFE was broken down into its individual components and each component was discussed in detail. The SAISAFE includes added subcomponents and elements that make it more relevant to the South African context.

The added subcomponents are Language, ICT Security Ombudsman, ICT Security Curriculum, and Information Repositories, as discussed in Sections 7.3.1 to 7.3.4. Lastly, all the building blocks that were identified from the models and frameworks were dealt with in detail in Sections 7.2.1 to 7.2.13.

# Chapter 8: Analysis and Findings

## 8.1 Introduction

The evaluation made in this research was based on exploratory testing and does not necessarily represent a complete testing of the framework. A pilot testing mechanism was employed using different focus groups that comprised of participants at the three academic conferences at which the research articles were presented.

As part of evaluating the validity and feasibility of the SAISAFE, it was included in the proceedings of three peer-reviewed international conferences. These conferences were used as focus groups for the evaluation and testing of the proposed framework. The conferences offered an opportunity for the research papers to be presented and peer-reviewed, and it also entailed receiving input and feedback from the audiences regarding the proposed framework. Hence, these conferences could be regarded as focus groups that participated in the evaluation of the proposed framework. The purpose of this chapter is to illustrate the evaluation of the SAISAFE by means of online questionnaires.

The online questionnaire was sent to both academic and industry experts. Eventually, eight experts were chosen because of their vast experience in the fields of ICT security, ICT security awareness, and ICT in Education. Another criterion for the selection of participants was the number of years that they had worked in their particular industry, as this would determine their level of experience.

The profiles of the eight participants are presented below, and due to a confidentiality agreement reached with them, their names cannot be divulged.

### **Participant 1**

An academic expert in e-education, she has been in the education industry as an educator, librarian, and innovator since 1973. Her qualifications include a National Diploma in Art Teaching and a Post Graduate Diploma in School Library Science. Some of her research interests are e-Learning, educational technology, curriculum development and design, and teacher training. She founded a number of education-based organisations that focus on younger school learners. She is a veteran in the South African education system, and has

worked for both the private sector and the public sector (the Department of Basic Education).

### **Participant 2**

This participant is a staunch academic who has been in the ICT industry for many years and is currently a Professor at the University of Fort Hare. His qualifications include a BSc, an MBA, and a doctoral degree from the Nelson Mandela Metropolitan University (NMMU). Over the past 12 years, he has authored and co-authored more than 70 reviewed publications and has worked for prominent institutions such as the CSIR, IBM, and SAP AG. Some of his research interests are Information Security, ICT in Education, E-learning, and statistics. His working experience includes working outside of South Africa in the private sector and many years in academia.

### **Participant 3**

This participant has been in the South African education system for many years. She founded a number of organisations (NGOs) that assist school learners against computer-related diseases. She has worked as a consultant at the Department of Basic Education. Some of her research interests include e-Learning, ICT in education, and ICT4D.

### **Participant 4**

This participant has been involved in the South African education system for many years. She holds a PhD from the University of South Africa. Her research interests are education management, ICT in education and ICT4D.

### **Participant 5**

This participant works as a lecturer the Tshwane University of Technology (TUT). She has been an academic and a lecturer at various tertiary institutions in South Africa for many years. Her research interests include ICT in Education, ICT4D, and ICT in general. She has a PhD in Information Technology.

### **Participant 6**

This participant has been involved in ICT most of his adult life. He has been involved in secondary school education for more than 40 years. He also worked as a director for E-

Learning and Library Services for the Western Cape Education Department. This participant started his Computer Science studies in 1979.

### **Participant 7**

This participant works as a professor at the Nelson Mandela Metropolitan University. His areas of expertise include software development, business intelligence, artificial intelligence, and information security. He has been in academia for many years and has authored and published many academic texts. He has also been a lecturer for many years and holds qualifications such as BSc, BTECH, MTECH, and a PhD.

### **Participant 8**

This participant is a lecturer and holds a PhD from the University of Fort Hare. Her research interests include Databases, Human-computer Interaction, Information Systems, Information Security and education. She has authored and co-authored a number of reviewed publications. She has worked for both government institutions and the private sector.

The participants have a vast number of years' experience in the spheres of both ICT security awareness and ICT in education. They have good academic backgrounds and have authored and co-authored numerous publications both in South Africa and internationally. It is for this reason that their views have been sourced and they were asked to participate in this research. The combined responses from the experts are summarised in Section 8.2.

## **8.2 Summary of the questions**

The subsections that follow were derived from the questions that were included in the questionnaire and that were subsequently completed by the experts. An analysis of the responses that were received was conducted and they are summarised by question. Each of the questions included in the questionnaire is presented as a sub-heading, followed by a discussion of the responses.

### 8.2.1 The problem with the integration of ICT into the South African education system

The participants confirmed that there is a problem with the integration of ICT into the South African education system. The responses to this question were categorised under different factors. Two respondents stated that the type of school (public or private) played a significant role in the integration of ICT in South African education. One respondent stated that private schools would have an advantage compared to public schools in this regard.

Insufficient basic ICT skills were also cited as a factor that deters this integration. One respondent stated that teachers often struggle with the usage of ICT. Two respondents mentioned the dangers associated with ICT. They further stated that teachers, learners and parents would have to be made aware of the dangers of ICT usage before it can be integrated in education. Another respondent mentioned that issues of privacy and security would have to be addressed if the integration of ICT into the South African education system were to be successful.

Inadequate support was mentioned as a factor that hampers integration. The respondent mentioned that the real challenge with integrating ICT in education involved support-related issues such as content development, teacher training, technical support, additional technical support staff on-site, etc. Another respondent mentioned a lack of understanding of the real issues that are at stake and jumping into conclusions without consulting the relevant stakeholders.

One of the respondents mentioned the curriculum as a problem in the integration of ICT into South African education. The respondent believes that what the school teaches learners is not what the industry requires. Two respondents stated that implementation also hinders the integration of ICT into education. One of the respondents mentioned a White Paper written in 2004 that was never properly implemented.

### 8.2.2 The advantages and disadvantages of the SAISAFE

The participants agreed that the proposed framework covers all aspects regarding ICT security awareness and education. They stated that the SAISAFE is holistic and easy to read.

However, three participants warned that the framework is too 'high-level' and that it does not communicate the necessary detail. One participant found the inclusion of language to be a positive aspect of the framework, while two others seemed to be confused as to why language was included in the framework.

The participants mentioned certain strengths and weaknesses of the questionnaire and the resulting framework.

As strengths, the participants suggested that the framework appears holistic and covers all aspect. They mentioned that it closes the existing gaps, and they liked the idea of including ICT security awareness in the curriculum. They supported the use of different languages. They stated that the SAISAFE was easy to read and agreed that it addressed many aspects regarding ICT in education. They also mentioned that the SAISAFE was comprehensive and included many elements that were necessary to implement ICT in the South African education system. They stated that the SAISAFE could be a useful tool for teaching learners to avoid becoming victims of ICT-related crime and believed that it could facilitate interactive learning among school learners.

As weaknesses (or disadvantages), one of the participants was concerned that the framework is 'high-level without implementation specifics'. One participant required more information in order to be able to respond to a particular question. Still another participant raised the concern that the framework was a mixed theoretical and practical model – they suggested that the framework be separated in order to distinguish between these two areas within the framework. A suggestion of the inclusion of teachers in the leadership component was made – as they would be the ones implementing the technology. Another participant questioned the inclusion of language as a building block and rather suggested the inclusion of components such as finance, human skills and access to technology. A participant claimed that ICT (especially the use of mobile phones) had become the teacher's enemy, and lastly, one of the participants referred to Operation Phakisa as a similar initiative.

### 8.2.3 The readability of the SAISAFE

Most participants found the framework easy to read. However, one of them stated that they found the framework difficult to understand. They stated that they would have preferred to attend a presentation before they were given the questionnaire. Another participant proposed a reshuffling of the components.

### 8.2.4 The viability of the SAISAFE

The participants agreed that the proposed framework addresses the lack of ICT security awareness in the South African education system. One participant stated that it was a start and that much more detail would be needed to address the problem. Another participant referred to the Department of Basic Education and Intel's programmes on e-safety. One participant mentioned that the framework would at least get people to start thinking about ICT security awareness in the South African schooling system. Another participant thought that the proposed framework addressed the lack of ICT security awareness – and that awareness must be prioritised, knowledge of problems and dangers must be emphasised, and ignorance must be addressed. The participant further stated that people were often too trusting and that they did not realise that learners might be tempted to access dangerous information on the internet.

### 8.2.5 Contribution of the SAISAFE to the quality of education in South Africa

The participants thought that the framework would make a positive contribution to the quality of education in South Africa. One participant noted that technology on its own cannot make a contribution but it can play a supportive role to improve the quality of education. They also stated that much more had to be done to improve the quality of teachers in terms of their content knowledge, approach to teaching, attitude, and dedication to the teaching profession. Another participant hoped that the framework would help create awareness and contribute towards integration and execution of ICT security awareness initiatives. They also mentioned that the collaboration and support process should be revised. Another participant stated that it would help if consultations with key

stakeholders such as provincial head offices and districts were held. Another participant stated that all depended on the implementation, because there are many visionaries but when it comes to implementation, such projects often fail to materialise.

### **8.2.6 Contribution of the SAISAFE towards integrating ICT security awareness into South African education**

Again the participants thought that the proposed framework would make a positive contribution towards the integration of ICT security awareness into the South African education system. However, one participant highlighted that teachers and schools would need to be prepared for ICT security awareness initiatives, and that very few were ready. Another participant's concern was how the proposed framework addressed issues such as technology integration during lessons. The responses in this subsection indicated that the participants generally thought the proposed framework would make a positive contribution towards the identified lack of integration of ICT security awareness into the South African education system.

### **8.2.7 Meaningful contribution to the overall South African education system**

The participants indicated that they thought the proposed framework would make a positive contribution towards the overall South African education system. One participant stated that very few schools and teachers were ready for integrating ICT security awareness at school, while another participant remarked that awareness needed to be emphasised. The responses that were received in this subsection indicated that the participants expected the proposed framework to make a positive contribution towards the overall South African education system.

### **8.2.8 Relevance of building blocks to South Africa**

The participants thought that the building blocks in the proposed framework were relevant and made a meaningful contribution to the final diagram. The relevance of these building blocks further confirmed the suitability and effectiveness of this framework.

### 8.2.9 Meaningful contribution of the SAISAFE to ICT Security Awareness in education

The participants expected the proposed framework to make a positive contribution to ICT security awareness in education. This means that the framework could make a meaningful contribution to the body of knowledge relating to ICT security awareness in education. One of the participants suggested that the word 'meaningful' had to be defined in this context.

### 8.2.10 Usage of the SAISAFE for future research

The participants agreed that the proposed framework could be used for future research. For instance, they suggested that the framework be implemented in practice over a period of time for future research. One of the participants further commented that the framework indeed provided some detail.

### 8.2.11 Implementation of the SAISAFE

The participants stated that should the framework be implemented, it would make people aware of the dangers of ICT usage. They also stated that appropriate teacher training had to be put in place. One participant emphasised that the incorporation of ICT security awareness into the curriculum was very important. They mentioned some institutions that could assist in this regard and argued that South African role players would have to be involved and consulted from the beginning. Another participant mentioned the need for consulting key stakeholders, including provincial head offices and districts. One participant stated that the framework needed a strong implementation structure and clear guidelines of procedures. They also mentioned that practical implementation and compliance would be essential for the success of the SAISAFE. Another participant believed that the safety of learners making use of ICT in the education system would be improved. Awareness had to be created among both the management and staff making use of the framework, so that they would put the necessary governance principles in place.

### 8.2.12 Overall rating of the SAISAFE

The participants rated the proposed framework positively. They stated that it made a good contribution towards the integration of ICT into the South African education system. One participant stated that for the SAISAFE to work, attitudes and behaviours would need to be considered as well.

### 8.2.13 Contribution made by formulating the proposed framework

The participants were satisfied that the formulation of the proposed framework was a positive contribution to the study field. One participant stated that the framework had big potential, but they would consider a few small changes.

## 8.3 Conclusion

This chapter discussed the results of the pilot study that was conducted. Each of the questions included in the online questionnaire was discussed and the responses of those questions (received from the participants) were included.

The online questionnaire was sent to ICT security experts both in academia and in the ICT industry, and they provided positive feedback as well as constructive criticism which were used to refine the proposed framework. The overall feedback and responses received from the experts indicated that the SAISAFE was viable, would make a meaningful contribution to the South African education system and was relevant to the South African context.

# Chapter 9: Conclusions and Future Research

## 9.1 Introduction

This chapter presents the conclusions reached in this research and discusses potential aspects of future research. Also, the research questions are revisited in this chapter to establish to what extent they have been addressed in this research.

## 9.2 Conclusions

An in-depth discussion was made of the South African ICT Security Awareness Framework for Education (SAISAFE). New components that were added, namely Language, ICT Security Ombudsman, ICT Security School Curriculum, and Information Repositories were thoroughly motivated and discussed, and it was agreed that these components would make the proposed framework (SAISAFE) more relevant to South Africa.

Even though there exist models and frameworks related to ICT security awareness in literature, there is still a gap when it comes to ICT security awareness models and frameworks that are specifically focused on South African school learners. The research in hand proposed a framework to integrate ICT security awareness into the South African schooling system.

The literature review that was conducted clearly showed that the models and frameworks encountered in the literature (see Section 6.2) do not cater for the challenges that are faced by South African school learners. Hence, South African school learners are at risk and vulnerable to ICT-related crimes. The literature review also made the author aware of the high number of ICT-related crimes in South Africa. This confirms the need to educate and inform not only the school learners, but also the population at large about the dangers posed by ICT usage.

The current research resulted in the proposal of a framework that is specific to South African school learners in the fight against ICT-related crimes and that assists with integrating ICT security awareness into the South African schooling system. The setting up of an ombudsman office for ICT-related crime in South Africa was also proposed and should be greatly beneficial to the victims of cyber-crime.

## 9.3 Future Research

Future research that can assist in drafting policies and procedures for use by the proposed ombudsman for ICT-related crimes in the country should be considered. For example, a research study should be conducted to help determine what needs to be done in future to ensure that these policies are created and implemented. Also, future research can assist with proposing the details of the curriculum that would be taught or made available at the proposed ICT training and learning centres. Another aspect that can be considered for future research is the formulation of a code of best practice document that will be used by all ICT stakeholders in South Africa, and, in particular, a proposal for a code of best practice for ICT security awareness in education throughout South Africa.

## 9.4 Re-visiting the Research Questions

The purpose of this subsection is to revisit the four research questions stated in Section 1.2.2 of this report. They are re-examined to determine whether the objectives of this research have been achieved. Each of the research questions are discussed below.

### 9.4.1 Can the existing models and frameworks be used for the integration of ICT security awareness into the South African education system?

The aim of this research question was to find out, through extensive literature review and analysis, whether the existing models and frameworks could be used to integrate ICT security awareness into the South African education system. The plan was to study literature and see whether any existing models and frameworks appropriately addressed this phenomenon.

An extensive literature review that studied literature related to both ICT security awareness and ICT-in-education was conducted. The review involved research where models and frameworks in both these two spheres were proposed. Many models and frameworks were studied and analysed.

Having studied and analysed many models and frameworks in literature, the researcher concluded that none of them could be used to integrate ICT security awareness into the South African education system. In fact, there was no model or framework that existed for this sole purpose. Therefore, the conclusion was reached that none of the existing models or frameworks could be successfully used to integrate ICT security awareness into the South African education system.

#### 9.4.2 Is there a gap between the ICT-in-education models and frameworks and the ICT security awareness models and frameworks?

As part of the literature review, an analysis was undertaken to find out if there was a gap between the two spheres of ICT security awareness and ICT in education. This analysis would help to determine if there was a need for a new framework that would be inclusive of both spheres.

After selecting the models and frameworks to be used in this research, an analysis-of-models-and-frameworks table was compiled to compare and analyse the two spheres. The table listed all the identified building blocks in the left-hand column of the table. The next three columns of the table contained ICT security awareness models and frameworks, while the last three presented the ICT-in-education sphere.

The analysis included checking whether a particular building block existed in both spheres and whether it existed in more than one model or framework. This analysis would help identify whether a gap existed between the two spheres and it solidified the notion that a framework to bridge this gap was indeed necessary.

#### 9.4.3 Which building blocks can be derived from existing models and frameworks to formulate and propose a framework that can be used for the integration of ICT security awareness into the South African education system?

This research question addressed the continuation of the literature review, but now with the aim of identifying the building blocks that could be used to formulate the proposed

framework. At this stage of the research, it was concluded that there was indeed a need for proposing a new framework.

Seeing that six models and frameworks (three in ICT security awareness sphere and three in ICT-in-education) were initially identified as useful to this research, the aim of this research question was to identify building blocks that could be used to formulate the proposed framework. These building blocks would be used as components of the new framework.

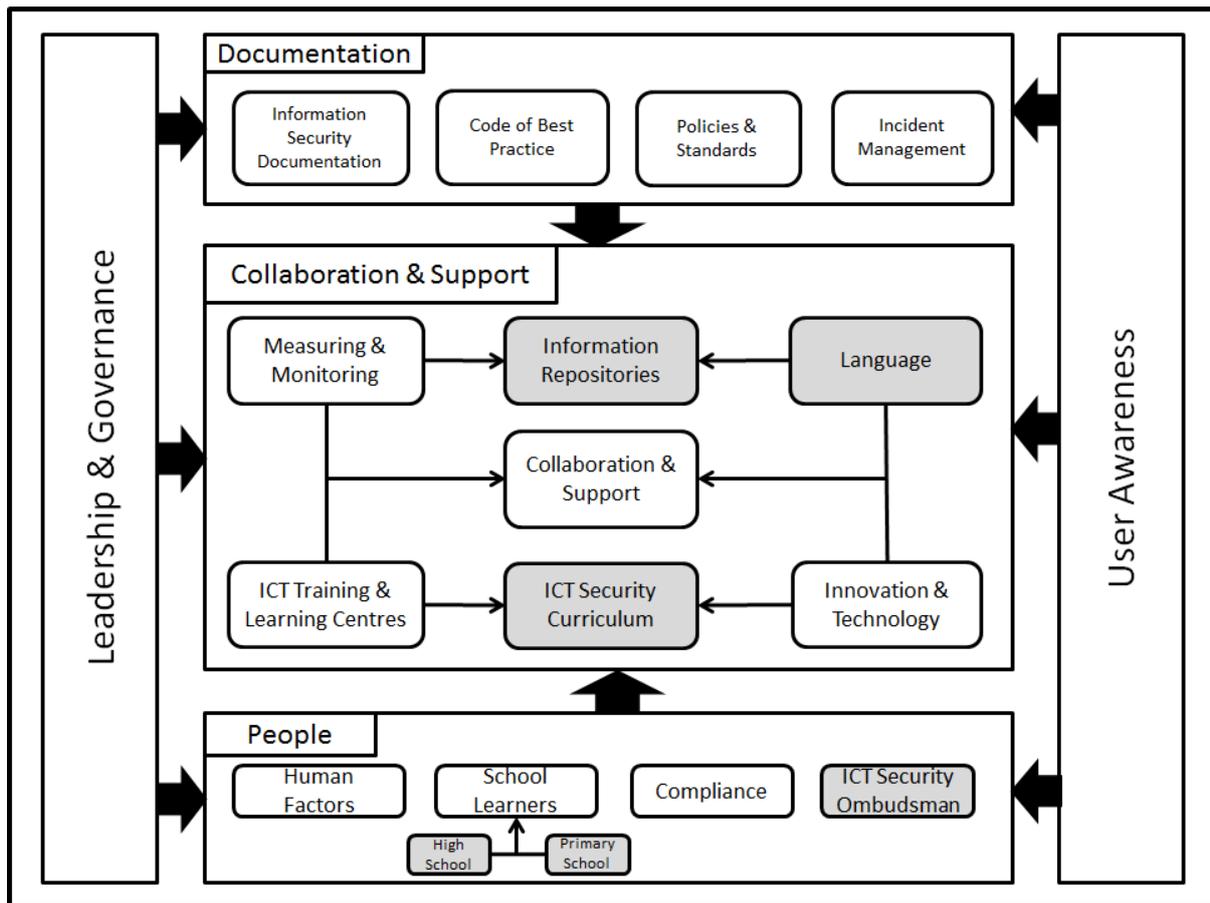
The criterion that was used to select the building blocks from the models and frameworks was quite simple. A component had to be relevant to South Africa and it also had to be closely related to the topic of this research. At some point, there were selected components that were repeating (or had similar meaning). This prompted the process of either combining them into one building block or simply eliminating one and using the other. After the selected components had been analysed, the total number of building blocks that would be used came down to 13. Each of the final building blocks that were selected through the iteration was discussed in Section 7.2.

#### 9.4.4 What framework can be used to integrate ICT security awareness into the South African education system?

This research question sought to find a framework to be proposed in this research. Having completed an extensive literature review, identified the building blocks, conducted the analysis of models and frameworks between the two spheres, and sent out online questionnaires to experts to validate the framework, the researcher formulated an appropriate framework for this research.

The framework was proposed based on all the building blocks as well as some of the suggestions that were received from the experts through the questionnaire responses. It bridged the gap between the two spheres because it was composed of building blocks that exist on both sides.

The framework proposed in this research was called the SAISAFE and, based on its exposition in Figure 9.1; it is evident that it can indeed be used to integrate ICT security awareness into the South African education system.



**Figure 9.1: The SAISAFE**

Figure 9.1 depicts the details of the framework proposed in this research. The SAISAFE can successfully be used to integrate ICT security awareness into the South African education system.

## 9.5 Contributions of this research

This section illustrates the contributions that have been achieved in this research and divides them into two subsections – academic contribution and practitioner contribution – with the aim of presenting both contributions distinctively.

### 9.5.1 Academic Contribution

From an academic point of view, this research identified two niche areas – ICT security awareness and ICT in education – and managed to bridge the identified gap between them. The literature review and the analysis of various models and frameworks resulted in the

identification of components that can be used to integrate ICT security awareness and ICT in education. The research found common ground between the two academic areas and this resulted in the formulation of a framework that can be used to integrate these two areas.

The proposed framework constitutes a new body of knowledge in ICT research. This new body of knowledge comprises of the integration between two spheres, namely ICT security awareness and ICT in education. The analysis of various models and frameworks to identify the gap that exists between the two spheres ensures that a major contribution is made by the way of formulating a suitable framework. Therefore, the main contribution of this research was the proposal of the SAISAFE. The framework was constructed through an in-depth literature review and an iterative process of identifying the relevant building blocks. These blocks, as well as their relevance to this research, were discussed in Section 7.2. The proposed framework is expected to stimulate the debate about the usage of ICT in the South African education schooling system. It raises relevant concerns that even though ICT usage has its benefits, it also has major disadvantages and limitations that need immediate attention. This research therefore proposes a framework that can be used to integrate ICT security awareness into the South African education system.

### 9.5.2 Practitioner Contribution

The practitioner contribution that is made by this research is a proposed framework to boost the discussion on ICT security awareness in the South African schooling system. It also provides an entry point that can be used by various stakeholders (such as the Department of Education) as a point of reference to introduce ICT security awareness into the South African school curriculum. Having received, reported and analysed the responses and feedback from the various experts who participated in the research, the researcher was able to present a more refined and improved framework.

Four “new” building blocks (themes) were identified through the in-depth literature review and the iterative process of selecting the relevant building blocks by using coding and themes. These building blocks were Language, ICT Security Ombudsman, ICT Security Curriculum, and Information Repositories. The contributions made by these “new” building blocks are discussed briefly below.

*Language:* A major contribution highlighted by this research is the proposal of using indigenous languages to reach a larger number of school learners in South Africa. Research has shown that it is better and easier to teach a person something if it is done in their home language (Roy, 2012). Thus, language is expected to play a major role in assisting with the integration of ICT security awareness into the South African education system.

*ICT Security Ombudsman.* Since this office does not exist in South Africa, its role will be to assist those who have been victims of ICT security-related crime. School learners as well as the general public will have a place where they can report ICT-related crime.

*ICT Security Curriculum.* The inclusion of ICT security awareness in the South African education system will ensure that school learners learn about ICT security awareness from a young age and therefore be more alert to ICT-related crime. This can stimulate and raise interest and awareness among school learners about the dangers of the usage of ICT devices such as smartphones, tablets, laptops, and many more.

*Information Repositories.* This research proposes the introduction of Information Repositories in public areas like hospitals, libraries, etc., all over South Africa. These information repositories will provide ICT security-related material that will equip both school learners and the general public to be ICT security aware.

The “new” building blocks that were discussed in this sub-section represent the practitioner contribution that has been made by this research.

## 9.6 Conclusion

This chapter investigated the conclusions reached in this research and made recommendations about future research in this field. The introduction in Section 9.1 was followed by a discussion of the conclusions and future research in Sections 9.2 and 9.3. In Section 9.4 the researcher revisited the research questions formulated prior to the study to show how and whether the research questions were solved. Section 9.5 was devoted to a discussion of the contributions made by this research.

# References

- Adedayo, W. S. and Ayobami, A. S. (2013) 'Relationship between information security awareness and information security threat', *INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT*, 3, pp. 115–119. Available at: <http://ssrn.com/abstract=2328542>.
- Ahmad, A. (2012) 'Type of Security Threats and It's Prevention.', *International Journal of Computer Technology & Applications*, 3(2), pp. 750–752. Available at: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Type+of+Security+Threats+and+It's+Prevention#0> (Accessed: 13 January 2015).
- Alnatheer, M. and Nelson, K. (2009) 'Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context', in *Proceedings of the 7th Australian Information Security Management Conference*. Security Research Institute Conferences. Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=ism>.
- Aloul, F. A. (2012) 'The Need for Effective Information Security Awareness', *Journal of Advances in Information Technology*, 3(3), pp. 176–183. doi: 10.4304/jait.3.3.176-183.
- Alper, Y. A. (2011) 'Controlling Insider Threats With Information Security Policies', in *ECIS 2011 Proceedings*, pp. 1–12.
- Amedzo, K. E. (2007) *The Integration of Information and Communication technology into Rural Schools of South Africa: A Case Study of Schools in Malamulele*. Stellenbosch University. Available at: <http://scholar.sun.ac.za/handle/10019.1/2135>.
- Andress, J. (2011) *The Basics of Information Security: Understanding the fundamentals of InfoSec in theory and practice*. Edited by Russ Rogers. Waltham: Syngress Press.
- Ashraf, S. (2005) 'Organization Need and Everyone's Responsibility Information Security Awareness', *The SANS Institute - Global Information Assurance Certification Paper*, (Security 401).
- Beckers, K., Heisel, M. and Hatebur, D. (2009) 'Supporting Common Criteria Security Analysis with Problem Frames\*', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(300266902), pp. 37–63.
- Belayneh, B. (no date) *South African Centre for Information Security*. Available at: <http://www.sacfis.co.za/index.htm> (Accessed: 14 June 2014).

- Bell ICT Solutions (2007) *The Benefits of ICT*. Available at:  
<http://www.bell.ca/web/enterprise/newsRoom/en/pdf/Benefits-of-ICT-White-Paper-EN.pdf>.
- Brownson, S. (2014) 'Student Experiential Learning of Cyber Security through Virtualization', *Journal of Research in Innovative Teaching*, 7(1), pp. 112–118.
- Bushati, J. et al. (2012) 'Advantages and Disadvantages of Using ICT in Education', in *International Conference in Europe*, pp. 1–17. Available at:  
[http://bederweb.majdanoz.net/Conferences/ICES 2012/FULL ARTICLE/Bushati\\_Barolli\\_Dibra\\_Haveri\\_Advantages and disadvantages of using ICT in education.pdf](http://bederweb.majdanoz.net/Conferences/ICES 2012/FULL ARTICLE/Bushati_Barolli_Dibra_Haveri_Advantages and disadvantages of using ICT in education.pdf).
- Chetty, J. and Coetzee, M. (2010) 'Towards an information security framework for service-oriented architecture', in *Information Security for South Africa*. IEEE, pp. 1–8. doi: 10.1109/ISSA.2010.5588272.
- Chi, M. (2011) 'Security Policy and Social Media Use'. The SANS Institute. Available at:  
<http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749>.
- Chigona, A. and Chigona, W. (2010) 'An Investigation Of Factors Affecting The Use Of ICT For Teaching In The Western Cape Schools', in *18th European Conference on Information Systems*, p. 12.
- Communications Security Establishment Canada (2013) 'Cyber Security Risks of Using Social Media Guidance for the Government of Canada', pp. 1–2.
- Creswell, J. W. (2009) *Research Design: Qualitative, Quantitative and Mixed Approaches (3rd Edition)*, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. doi: 10.2307/1523157.
- Department of Communications (2010) 'The South African Cyber Security Policy', *Government Gazette*, pp. 1–16. doi: <http://dx.doi.org/9771682584003-32963>.
- Department of Communications (2014) 'National Integrated ICT Policy Green Paper', *Government Gazette*, 24 January, pp. 3–104. Available at: [www.gpwonline.co.za](http://www.gpwonline.co.za).
- Department of Education (2004) 'White Paper on e-Education'. *Government Gazette*, pp. 3–

46. Available at:

<http://www.education.gov.za/LinkClick.aspx?fileticket=Keu0%2FBkee%2BM%3D&tabid=191&mid=484>.

Department of Education (2007) 'Guidelines for Teacher Training and Professional Development in ICT'.

Dlamini, Z. and Modise, M. (2012) 'Cyber Security Awareness Initiatives in South Africa: A Synergy Approach', in *7th International Conference on Information Warfare and Security*. Seattle, USA: Academic Conferences International, pp. 62–83. doi: 10.1007/978-3-8349-4134-3\_3.

Dlodlo, N. (2009) 'Access to ICT education for girls and women in rural South Africa: A case study', *Technology in Society*. Pretoria, 31(2), pp. 168–175. doi: doi:10.1016/j.techsoc.2009.03.003.

Draper, K. (2010) *Understanding science teachers' use and integration of ICT in a developing country context*. University of Pretoria. Available at:

<http://upetd.up.ac.za/thesis/available/etd-02032011-132142/unrestricted/thesis.pdf>.

Drevin, L., Kruger, H. A. and Steyn, T. (2007) 'Value-focused assessment of ICT security awareness in an academic environment', *Computers & Security*, 26(1), pp. 36–43. doi: 10.1016/j.cose.2006.10.006.

Edwards, C. K. (2013) *A Framework for the Governance of Information Security, Computers & Security*. Nova Southeastern University. Available at:

<http://www.sciencedirect.com/science/article/pii/S0167404804002639> (Accessed: 26 January 2015).

Fibikova, L. and Mueller, R. (2012) 'Threats, Risks and the Derived Information Security Strategy', in *Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference (2012)*. Daimler Northeast Asia Ltd, pp. 11–20. doi: 10.1007/978-3-658-00333-3\_2.

Ford, M. and Botha, A. (2010) 'A Pragmatic Framework for Integrating ICT into Education in South Africa', in Paul Cunningham and Miriam Cunningham (ed.) *IST-Africa 2010 Conference Proceedings*. Port Elizabeth: IIMC International Information Management Corporation, pp.

1–10.

Fourie, L. and McNamara (2008) *Enhancing the Livelihoods of the Rural Poor Through ICT: A Knowledge Map, South Africa Country Study*. 13. Available at: [http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037\\_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf](http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf).

Francis, L.-A. (2010) *DOC prioritises cyber security*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=34338:doc-prioritises-cyber-security](http://www.itweb.co.za/index.php?option=com_content&view=article&id=34338:doc-prioritises-cyber-security) (Accessed: 14 June 2014).

Fu, J. S. (2013) 'ICT in Education : A Critical Literature Review and Its Implications', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 9(1), pp. 112–125.

Gillwald, A., Moyo, M. and Stork, C. (2012) 'What is happening in ICT in South Africa: A supply-and demand-side analysis of the ICT sector', *Evidence for ICT Policy Action*. Research ICT Africa, (7). Available at: <http://www.researchictafrica.net/docs/Policy Paper 7 - Understanding what is happening in ICT in South Africa.pdf>.

Gokhe, M. (2000) 'Concept of Information, Communication and Educational Technology', *Thakur Shyamnarayan College of Education and Research (TSCER)*, p. 81. Available at: [http://www.tscermumbai.in/resources\\_paper\\_4/IV.1\\_information\\_and\\_communication\\_technology.pdf](http://www.tscermumbai.in/resources_paper_4/IV.1_information_and_communication_technology.pdf).

Government of the Hong Kong Special Administrative Region (2008) *An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region*. Hong Kong. Available at: <http://www.infosec.gov.hk/english/technical/files/overview.pdf>.

Grobler, M., Vuuren, J. J. Van and Leenen, L. (2012) 'Implementation of a Cyber Security Policy in South Africa : Reflection on Progress and the Way Forward Current State of Cyber Security Research in South Africa', in *ICT Critical Infrastructures and Society*. Amsterdam: Springer Berlin Heidelberg, pp. 215–225. doi: 10.1007/978-3-642-33332-3\_20.

Grobler, M., Vuuren, J. J. Van and Zaaiman, J. (2011) 'Evaluating Cyber Security Awareness in South Africa', *10th European Conference on Information Warfare and Security ECIW-2011*,

pp. 113–121.

Gundemeda, N. (2014) 'Information Technology (IT) Education in Andhra Pradesh: A Sociological View', *Journal of Social Sciences*, 40(3), pp. 333–342. Available at: [http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemeda-N/JSS-40-3-333-14-1567-Gundemeda-N-Tx\[5\].pdf](http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemeda-N/JSS-40-3-333-14-1567-Gundemeda-N-Tx[5].pdf) (Accessed: 2 October 2014).

Gundu, T. and Flowerday, S. V (2013) 'Ignorance to Awareness: Towards an Information Security Awareness Process', *SAIEE Africa Research Journal*, 104(2), pp. 69–79.

Hancock, B., Ockleford, E. and Windridge, K. (2009) 'An Introduction to Qualitative Research', *The NIHR RDS EM/YH*. Available at: <http://books.google.cz/books?id=sFv1oWX2DoEC>.

Higgins, S. (2003) 'Does ICT Improve Learning and Teaching in Schools?', *Journal of Science and Technology*. Bera, 17(6), pp. 586–594. Available at: <http://www.bera.ac.uk/files/reviews/ict-pur-mb-r-f-p-1aug03.pdf>.

Hong, K. S. and Songan, P. (2011) 'ICT in the changing landscape of higher education in Southeast Asia', *Australasian Journal of Educational Technology*, 27(8), pp. 1276–1290. doi: 10.14742/ajet.893.

Information Security Resource Center (no date) *Basic Information Security Principles*. Available at: [http://www.oregon.gov/DAS/CIO/ISRC/pages/intro\\_basics.aspx](http://www.oregon.gov/DAS/CIO/ISRC/pages/intro_basics.aspx).

Internet Service Provider's Association (no date) *419 Scams*. Available at: <http://ispa.org.za/spam/419-scams/>.

ISACA (2009) *An Introduction to the Business Model for Information Security*. ISACA. Available at: <http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>.

Isisag, K. U. (2012) 'The Positive Effects of Integrating ICT in Foreign Language Teaching', in *ICT for Language Learning*. Available at: [http://conference.pixel-online.net/ICT4LL2012/common/download/Paper\\_pdf/235-IBT107-FP-Isisag-ICT2012.pdf](http://conference.pixel-online.net/ICT4LL2012/common/download/Paper_pdf/235-IBT107-FP-Isisag-ICT2012.pdf).

Jabareen, Y. (2009) 'Building a conceptual framework: philosophy, definitions, and procedure', *International Journal of Qualitative Methods*, 8, pp. 49–62. doi: 10.2522/ptj.20100192.

- John, V. (2015) *Education MEC promises to take Gauteng classrooms into the future*, *Mail&Guardian*. Available at: <http://mg.co.za/article/2015-05-20-education-mec-promises-to-take-gauteng-classrooms-into-the-future> (Accessed: 27 August 2015).
- Johnson, M. (2012) 'Cybercrime: Threats and Solutions', *Available at SSRN*. Ark Group. Available at: <http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf> (Accessed: 13 January 2015).
- Kabay, M. E. (2002) 'What's Important for Information Security: A Manager's Guide'. Northfield: Norwich University, pp. 1–4.
- Kayle, A. (2011) *SA's security awareness lags*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=42395](http://www.itweb.co.za/index.php?option=com_content&view=article&id=42395).
- Kortjan, N. and Von Solms, R. (2014) 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal*, 52, pp. 29–41. Available at: <http://sacj.cs.uct.ac.za/index.php/sacj/article/view/201/95>.
- Kreutzer, T. (2009) 'Assessing Cell Phone Usage in a South African Township School', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*. Cape Town: e/merge, 5(5), pp. 43–57. Available at: <http://emerge2008.net>.
- Kritzinger, E. (2006) *An Information Security Retrieval And Awareness Model For Industry*. University of South Africa. Available at: <http://uir.unisa.ac.za/bitstream/handle/10500/2475/thesis.pdf?sequence=1>.
- Kritzinger, E. and Padayachee, K. (2007) 'Teaching Safe and Secure usage of ICTs in South African Schools', in *Proceedings of the 2nd International Conference on Society and Information Technologies*. Pretoria, pp. 1–6. Available at: <http://hdl.handle.net/10500/3986>.
- Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security*. Elsevier Ltd, 29(8), pp. 840–847. doi: 10.1016/j.cose.2010.08.001.
- Kruger, H. A., Drevin, L. and Steyn, T. (2006) 'A Framework For Evaluating ICT Security Awareness', in *Information Security for South Africa*, pp. 1–11.
- Kruger, H. a. and Kearney, W. D. (2008) 'Consensus ranking – An ICT security awareness case

- study', *Computers & Security*. Elsevier Ltd, 27(7–8), pp. 254–259. doi: 10.1016/j.cose.2008.07.001.
- Kyobe, M. (2010) 'Towards a framework to guide compliance with IS security policies and regulations in a university', in *Information Security for South Africa*. Ieee, pp. 1–6. doi: 10.1109/ISSA.2010.5588651.
- Kyobe, M. E., Molai, P. and Salie, T. (2009) 'Investigating electronic records management and compliance with regulatory requirements in a South African university', *SA Journal of Information Management*, 11(1), pp. 1–15. doi: 10.4102/sajim.v11i1.396.
- De Lange, M. and Von Solms, R. (2013) 'An e - Safety Educational Framework in South Africa', in *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Cape Town, p. 497. Available at: [http://www.satnac.org.za/proceedings/2012/papers/3.Internet\\_Services\\_End\\_User\\_Applications/53.pdf](http://www.satnac.org.za/proceedings/2012/papers/3.Internet_Services_End_User_Applications/53.pdf).
- Lau, K. and Albion, P. R. (2010) 'Hong Kong Home Economics Teachers' Adoption of ICT for Learning and Teaching', in Romeo, G. and Gronn, D. (eds) *Digital Diversity Australian Computers in Education Conference 2010*. ACCE. Available at: <http://eprints.usq.edu.au/7354/>.
- Liu, Z., Shu, G. and Lee, D. (2011) *Network Security, Administration and Management*. Edited by D. C. Kar and M. R. Syed. IGI Global. doi: 10.4018/978-1-60960-777-7.
- Maholwana-Sotashe, N. L. (2007) *Challenges faced by secondary school teachers in integrating ICT into the curriculum: A multiple case study in the Grahamstown Circuit*. Rhodes University.
- Mdlongwa, T. (2012) 'Information and Communication Technology ( ICT ) as a Means of Enhancing Education in Schools in South Africa : Challenges , Benefits and Recommendations'. Pretoria: Africa Institute of South Africa, pp. 1–8.
- Mikre, F. (2011) 'The Roles of Information Communication Technologies in Education Review Article with Emphasis to the Computer and Internet', *Ethiopian Journal of Education and Sciences*, 6(2). Available at: <http://www.ajol.info/index.php/ejesc/article/view/73521/62437>.

---

Miller, L., Naidoo, M. and Belle, J. Van (2003) 'Critical Success Factors for ICT Interventions in Western Cape Schools'. Cape Town: Department of Information Systems, University of Cape Town, pp. 1–14.

Minister of Justice and Correctional Services (2017) *Cybercrimes and Cybersecurity Bill*. Republic of South Africa. doi: -.

Moll, I. *et al.* (2007) 'Status Report on ICTs and Higher Education in South Africa'. Braamfontein: South African Institute for Distance Education (SAIDE). Available at: [http://www.judybackhouse.com/pdfs/saide\\_status\\_of\\_elearning\\_in\\_sa.pdf](http://www.judybackhouse.com/pdfs/saide_status_of_elearning_in_sa.pdf).

Mullamaa, K. (2010) 'ICT in Language Learning--Benefits and Methodological Implications', *International Education Studies*, 3(1), pp. 38–44. Available at: <http://www.ccsenet.org/journal/index.php/ies/article/view/4965/4131>.

MyBroadband (2014) *SA students pour R6.1 billion into tech*. Available at: <http://businesstech.co.za/news/general/55685/sa-students-pour-r6-1-billion-into-tech/>.

Mzekandaba, S. (2015) *Cybercrime cost SA over R3.42bn in 2013*, *ITWeb Africa*. Available at: <http://www.itwebafrica.com/security/514-south-africa/234087-cybercrime-cost-sa-over-r342bn-in-2013> (Accessed: 15 March 2015).

Ndlovu, N. S. and Lawrence, D. (2012) 'The quality of ICT use in South African classrooms', in *Towards Carnegie III*. Cape Town: University of Cape Town.

Nevondwe, L. and Odeku, K. O. (2014) 'Protecting Children from Exposure to Pornography in South Africa', *Bangladesh e-Journal of Sociology*, 11(2), pp. 132–142.

Ngcobo, M. (2009) 'A strategic promotion of language use in multilingual South Africa: information and communication', *Southern African Linguistics and Applied Language Studies*, 27(1), pp. 113–120. doi: 10.2989/SALALS.2009.27.1.9.757.

Nyakowa, S. L. (2014) *Factors Influencing ICT Adoption Among Public Secondary School Teachers : A Case of Webuye Sub-County, Bungoma County, Kenya*. University of Nairobi.

Oates, B. J. (2011) *Researching Information Systems and Computing*. London: Sage Publications Ltd.

Olivier, M. S. (2004) *Information Technology Research: A practical guide for Computer Science and Informatics*. 2nd edn. Pretoria: Van Schaik Publishers.

- Ope, J. (2014) *An Information Systems Security Framework for Kenyan Public Universities*. University of Nairobi. Available at: <http://erepository.uonbi.ac.ke/handle/11295/76933> (Accessed: 20 January 2015).
- Plessis, A. and Webb, P. (2012) 'A Teacher Proposed Heuristic For ICT Professional Teacher Development and Implementation In The South African Context', *Turkish Online Journal of Educational Technology*, 11(4), pp. 46–55.
- Poepjes, R. and Lane, M. (2012) 'An Information Security Awareness Capability Model (ISACM )', in *Australian Information Security Management Conference*. Edith Cowan University Research Online. Available at: <http://ro.ecu.edu.au/ism/137>.
- PriceWaterhouseCoopers (2010) *Information and Communication Technology for Education in India and South Asia, ICT in School Education (Primary and Secondary)*. Available at: [http://www.infodev.org/infodev-files/resource/InfodevDocuments\\_1016.pdf](http://www.infodev.org/infodev-files/resource/InfodevDocuments_1016.pdf).
- Qureshi, I. A., Whitty, M. and Whitty, M. (2014) 'Facebook as e-learning tool for higher education institutes', *Knowledge Management & E-Learning*, 6(4), pp. 440–448.
- Radovanovic, D., Radojević, T. and Sarac, M. (2010) 'IT audit in accordance with Cobit standard', in *MIPRO, 2010 Proceedings of the 33rd International Convention*. Opatija, Croatia: IEEE Xplore, pp. 1137–1141. Available at: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5533627](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5533627).
- Romm, N. R. A. and Phil, D. L. (2013) 'Employing Questionnaires in terms of a Constructivist Epistemological Stance: Reconsidering Researchers' Involvement in the Unfolding of Social Life', *International Journal of Qualitative Methods*, pp. 652–669.
- Rotich, D. C. and Munge, E. M. (2007) 'An overview of electronic information resources sharing initiatives in Kenyan universities', *SA Jnl Libs & Info Sci*, 73(1), pp. 64–74.
- Rowe, D. C., Lunt, B. M. and Ekstrom, J. J. (2011) 'The role of cyber-security in information technology education', *Proceedings of the 2011 conference on Information technology education - SIGITE '11*. New York, New York, USA: ACM Press, 2, p. 113. doi: 10.1145/2047594.2047628.
- Roy, A. *et al.* (2014) 'Promoting proper education for sustainability: An exploratory study of ICT enhanced Problem Based Learning in a developing country', *International Journal of*

- Education and Development using Information and Communication Technology*, 10(1), pp. 70–90.
- Roy, N. K. (2012) 'ICT-Enabled Rural Education in India', *International Journal of Information and Education Technology*, 2(5), pp. 525–529. doi: 10.7763/IJiet.2012.V2.196.
- Saleh, Z. I., Heba, R. and Mashhour, A. (2011) 'Proposed Framework for Security Risk Assessment', *Journal of Information Security*, 02(02), pp. 85–90. doi: 10.4236/jis.2011.22008.
- Saunders, M., Lewis, P. and Thornhill, A. (2008) *Research Methods for Business Students*, *Research methods for business students*. doi: 10.1007/s13398-014-0173-7.2.
- Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students*. Pearson Education Limited.
- Smit, D. (2015) 'Cyberbullying in South African and American schools: A legal comparative study', *South African Journal of Education*, 35(2), pp. 1–11. doi: 10.15700/saje.v35n2a1076.
- Smith, E. H. and Kruger, H. A. (2010) 'A framework for evaluating IT security investments in a banking environment', in *Information Security for South Africa*. Sandton: IEEE, pp. 1–7. doi: 10.1109/ISSA.2010.5588343.
- Von Solms, S. and Von Solms, R. (2014) 'Towards Cyber Safety Education in Primary Schools in Africa', in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, pp. 185–197.
- Straker, L. *et al.* (2010) 'Evidence-based guidelines for the wise use of computers by children: physical development guidelines.', *Ergonomics*, 53(4), pp. 458–77. doi: 10.1080/00140130903556344.
- Straker, L., Pollock, C. and Maslen, B. (2009) 'Principles for the wise use of computers by children.', *Ergonomics*, 52(11), pp. 1386–401. doi: 10.1080/00140130903067789.
- Surty, M. E. (2011) 'Quality education for rural schools in South Africa – challenges and solutions', *South African Rural Educator*. South Africa: Department of Basic Education, pp. 8–15.
- Swanepoel, A. J. (2015) *Towards A Framework For Understanding Information Systems*. University of Pretoria. doi: 2263/50796.

- The European Network and Information Security Agency (ENISA) (2010) *The new users' guide: How to raise information security awareness*. Available at:  
[http://www.enisa.europa.eu/publications/archive/copy\\_of\\_new-users-guide](http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide).
- UNESCO (2012) 'Why Language Matters for the Millenium Development Goals', in *Language, Education and the Millennium Development Goals*. Bangkok: UNESCO Bangkok.
- UNICEF (2012) 'South African mobile generation. Study on South African young people on mobiles', pp. 1–47. doi:  
[http://www.unicef.org/southafrica/SAF\\_resources\\_mobilegeneration.pdf](http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf).
- Da Veiga, A. (2008) *Cultivating and Assessing Information Security Culture*. University of Pretoria. doi: <http://hdl.handle.net/2263/24117>.
- Venktesh, K. (2016) *SA falls in key global ICT index, fintech24*. Available at:  
<http://www.fin24.com/Tech/News/sa-falls-in-key-global-ict-index-20161122> (Accessed: 15 May 2017).
- Veríssimo, P. and Rodrigues, L. (2001) 'Fundamental Security Concepts', in *Distributed Systems for System Architects*. Springer US, pp. 377–393. doi: 10.1007/978-1-4615-1663-7\_16.
- Vermeulen, J. (2014a) *Critical security bug gets SA sites, hosts scrambling, mybroadband*. Available at: <http://mybroadband.co.za/news/security/100324-critical-security-bug-gets-sa-sites-hosts-scrambling.html>.
- Vermeulen, J. (2014b) *New online banking fraud scheme in South Africa, mybroadband*. Available at: <http://mybroadband.co.za/news/general/100368-new-online-banking-fraud-scheme-in-south-africa.html>.
- Walaza, M., Loock, M. and Kritzinger, E. (2014) 'A Framework to Integrate ICT Security Awareness into the South African Schooling System', in *SAICSIT '14 Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology*. Pretoria: ACM, p. 11. doi: 10.1145/2664591.2664596.
- Walaza, M., Loock, M. and Kritzinger, E. (2015) 'A Pragmatic Approach towards the Integration of ICT Security Awareness into the South African Education System', in *The*

*Second International Conference on Information Security and Cyber Forensics (InfoSec2015)*. Cape Town, pp. 35–40.

Wayman, I. and Kyobe, M. (2012) 'Incorporating Knowledge of Legal and Ethical Aspects into Computing Curricula of South African Universities', *Journal of Information Technology Education: Innovations in Practice*, 11.

Whitman, M. E. and Mattford, H. J. (2011) *Road Map To Information Security: For IT And InfoSec Managers*. Boston: Course Technology.

# Appendices

## Appendix A: Accepted Research Article – SAICSIT2014

### **A Framework to Integrate ICT Security Awareness into the South African Schooling System**

Mvelo Walaza, Marianne Loock, Elmarie Kritzinger

School of Computing

University of South Africa

Pretoria, South Africa

53315804@mylife.unisa.ac.za, loockm@unisa.ac.za, kritze@unisa.ac.za

#### **ABSTRACT**

In various countries, information and communication technology (ICT) is used to enhance and improve the levels and standards of education. Scholars in countries such as South Africa have conducted studies to prove that ICT can be essential in the improvement and enhancement of education. This study deals with the problem of the lack of ICT security awareness in South African education (among South African learners). Research studies that have been conducted have shown that there is a huge problem when it comes to integrating ICT security awareness into the South African schooling system. With the resurgence of new technologies such as Facebook, Twitter and Skype, school learners are more vulnerable to ICT security attacks and ICT-related crime than ever before. Even though the studies, models and frameworks have been conducted and proposed, there is still a gap when it comes to solutions that are directed specifically to South African school learners. Hence a more integrated approach in the form of a framework, directed mostly on South African school learners, has been proposed in this study. In this study, an in-depth literature review of past scholarly work, models and frameworks is done. Having reviewed some of the existing models and frameworks, and identified the potential gaps, a framework to address the aforementioned problem is proposed. The results of the literature review analysis and the proposed framework are reported and compared to support the gap analysis.

#### **Keywords**

ICT, education, models, frameworks, security, awareness, school learners.

#### **INTRODUCTION**

According to Belayneh (Belayneh, no date), South Africa is at a crisis point when it comes to ICT security and drastic measures need to be taken. Craig Rosewarne (founder of ISG Africa), as cited by Kayle (Kayle, 2011), states that South Africa is lagging behind when it comes to information security awareness when compared to both Africa and its international counterparts. Rosewarne (Kayle, 2011) further highlights that South Africa does not have an incident response team that the whole country can use, and stresses the importance of forming partnerships to deal with cyber-crime in the country.

Even though ICT is used across all spheres of the industry in South Africa, recent research has shown that school learners are amongst the highest and most frequent users of ICT (MyBroadband, 2014). With children being one of the most vulnerable groups in South Africa due to the high crime rates, it is of utmost importance that they are well informed about ICT security. School learners (as seen on the news) are facing dangers such as human-trafficking, rape, kidnapping, cyber-bullying, and many more in South Africa on a daily basis. The perpetrators of these crimes can use all avenues to gather information about their victims. Hence the school learners must be made aware of the importance of ICT security.

The in-depth literature review that has been conducted has enabled the researcher to identify a gap in the existing models and to formulate a hypothesis. A gap analysis of the existing models and frameworks will be done and based on the findings of the research, a framework will be proposed as a solution to the research problem.

In this article, an in-depth literature review is conducted in section 2, in which the current usage of ICT in South Africa is discussed. However, the main aim of this research article is to look at the existing models and frameworks in literature and then to formulate and propose a framework that is more specific to the South African education system and environment. The findings will be discussed and explained, and then lastly, the conclusions made from the article will be discussed.

## **LITERATURE REVIEW**

This section looks at the current ICT usage in South Africa, the ICT usage in South African education including the benefits and challenges thereof, ICT safety and security, ICT security awareness in general, and ICT security awareness in education.

### **ICT usage in South Africa**

South Africa has the characteristics of both a developing and an advanced economy. It has access to a lot of technologies, research institutions, universities, private and governmental organisations that have good resources. Amazingly, more than half of the population still live below the poverty line and these anomalies are clearly evident in the South African ICT sector (Gillwald, Moyo and Stork, 2012).

The South African Department of Communications, which is the main custodian of ICT in the country, has written a Green Paper in which it states that its purpose is to change and improve the ICT sector and the country's economy (Department of Communications, 2014). It states that the country has not yet taken advantage of the possibilities and opportunities that are created by the digitisation and convergence of communication technologies. The Department of Communications' Green Paper says that the communications industry in South Africa is divided into telecommunications, broadcasting and postal services (Department of Communications, 2014).

### **The benefits and challenges of ICT usage in South African education**

With the advancement and availability of technology around the world, one would expect a certain level of the usage of ICT in South African schools. It is disappointing to learn that some educators in South African schools are still using ICT merely to transmit subject content instead of using it to improve learning (Ndlovu and Lawrence, 2012). However, the Department of Education has realised that the importance of the integration of ICT in education can no longer be ignored (Amedzo, 2007). This has resulted in the Department of Education including information technology (IT) in their curriculum. The Department of Education (Department of Education, 2004) has released a White Paper to facilitate the introduction of e-Education in South African schools.

Some of the benefits of using ICT in education are, among others, the enhancement of collaboration and motivation among learners and the improvement of skills and knowledge among educators and learners (Mdlongwa, 2012)(PriceWaterhouseCoopers, 2010). Mdlongwa (Mdlongwa, 2012) further mentions more benefits as the enhancement of both active participation in the classroom and self-esteem among the school learners.

A challenge mentioned by Mikre (Mikre, 2011) is the misuse of technology by school learners. Instead of using ICT for learning purposes, school learners use technology for leisure activities such as online gaming and social networks (including Facebook and Twitter). Some of the challenges to the implementation of ICT in schools are the high cost of technology implementation and maintenance, fear of change among the educators, and the language used. Most software packages are written in English, which is not a mother tongue to most learners and educators (Mdlongwa, 2012). Section 2.3 discusses ICT safety and security.

### **ICT safety and security**

In a world where ICT has become so vital and invaluable (The European Network and Information Security Agency (ENISA), 2010), information security has become increasingly important for the success of many businesses (Edwards, 2013). A large number of people in different countries worldwide use their laptops in coffee shops, do internet banking using their mobile phones, and sometimes do their online shopping while sitting at home using unsecured computers and networks (Gillwald, Moyo and Stork, 2012).

### **ICT security awareness**

ICT security awareness is not training, but is an attempt to change the behaviour and patterns of how employees of an organisation and the general public use technology and the internet (The European Network and Information Security Agency (ENISA), 2010). Because we live in a world where the internet has become a part of millions of people's everyday lives (Kritzinger and Von Solms, 2010), ICT security awareness is of utmost importance. The internet is not only being used by businesses, but it is also being used extensively by home users doing tasks such as shopping online, online banking, searching for information and many more.

### **ICT security awareness in South African education**

As alluded by Rowe et al (Rowe, Lunt and Ekstrom, 2011), given the number of technologies used these days, it is not an ideal situation for school learners to have minimal knowledge and awareness of information security. In most academic institutions school learners usually

do their work (assignments and projects) using desktop computers that are connected to the network. This means that the unavailability of these resources may lead to loss of work and school work not being completed on time (Drevin, Kruger and Steyn, 2007).

Padayachee and Kritzinger (Kritzinger and Padayachee, 2007) state that four basic safety and security concerns for children have been identified when it comes to ICT usage. These safety and security concerns include information security risks (malware, spam, identity theft, etc), physical risks (musculoskeletal discomfort, visual problems, etc), personal social impact risks (withdrawal, internet addiction, etc), and interaction threats (internet predation, cyber-bullying, etc). These issues and concerns and the growing usage of ICT by school children in South Africa have caused Padayachee and Kritzinger (Kritzinger and Padayachee, 2007) to suggest and propose the inclusion of e-safety and information security in the South African school curriculum.

## **RESEARCH METHODOLOGY**

This section looks at the problem statement, the research questions, the research objectives and the research methodology used.

### **Problem statement**

In their research study, Padayachee and Kritzinger (Kritzinger and Padayachee, 2007) investigated the possibility of the inclusion of e-safety and information security in the South African school curriculum. This and many other reasons have led one to conclude that there is still a lack of integration of ICT security awareness in the South African education. The problem statement for this research study is as follows:

- The lack of integration of ICT security awareness in South African education

The problem statement looks at the integration of ICT security awareness, specifically into the South African schooling system. The research questions for this research article are discussed in section 3.2 below.

### **Research questions, objectives and deliverables**

As a result of the lack of ICT security awareness in South African education, Padayachee and Kritzinger (Kritzinger and Padayachee, 2007) say that it is very important that school

children are introduced and taught about information security at an early stage of their lives. The following research question aims to ensure that this can be accomplished.

- What framework can be used to integrate ICT security awareness into the South African schooling system?

This research question has been formulated in an attempt to find a solution to the problems encountered in South African schools. In response to the research question that has been mentioned, the research objective of this article is as follows:

- To propose a framework that can be used to integrate ICT security awareness into the South African schooling system

After the thorough data-gathering process has been completed using the methods mentioned in the research objectives, the next step is to discuss the research deliverables of the research article. Based on the findings from the in-depth literature review, the solution will be a proposed framework to integrate ICT security awareness in the South African schooling system.

### **Research methodology**

An in-depth literature review was conducted. This literature review is based on related academic papers within the ICT security awareness field. Scholarly work done by peers in the related field of study will also be reviewed and used if necessary. All the information gathered and used will be properly referenced and credit will be given to the authors where necessary.

The researcher has chosen to do a gap analysis of existing models and frameworks in literature in order to formulate and propose a framework that is specific to the South African schooling system. Various building blocks will be identified and analysed with the aim of formulating the proposed framework. Each framework and model will be analysed and various building blocks will be identified. The building blocks that will be identified will be used to formulate the proposed framework of this research article.

One of the main goals of this research is to improve the standard of education in South African schools with the usage of ICT. As literature has shown that one of the problems in

schools is the lack of ICT security awareness, this research aims to assist with overcoming this problem. Various models and frameworks used to assist with ICT security in South African schools were discussed in the previous sections. However, the researcher feels that these models and frameworks have not specifically addressed the problem at hand. This research study will propose a framework that will aim to address the problem of the lack of information security awareness in South African schools.

### ICT SECURITY MODELS AND FRAMEWORKS

A number of ICT security models and frameworks have been published and exist in scholarly literature. These models and frameworks refer to a number of important aspects of ICT in education, ICT security and ICT security awareness in general.

#### ICT security models

This subsection discusses ICT security models that exist in literature. These models will be used as the building blocks for the proposed model. Figure 1 depicts the Comprehensive Information Security Framework (CISF).

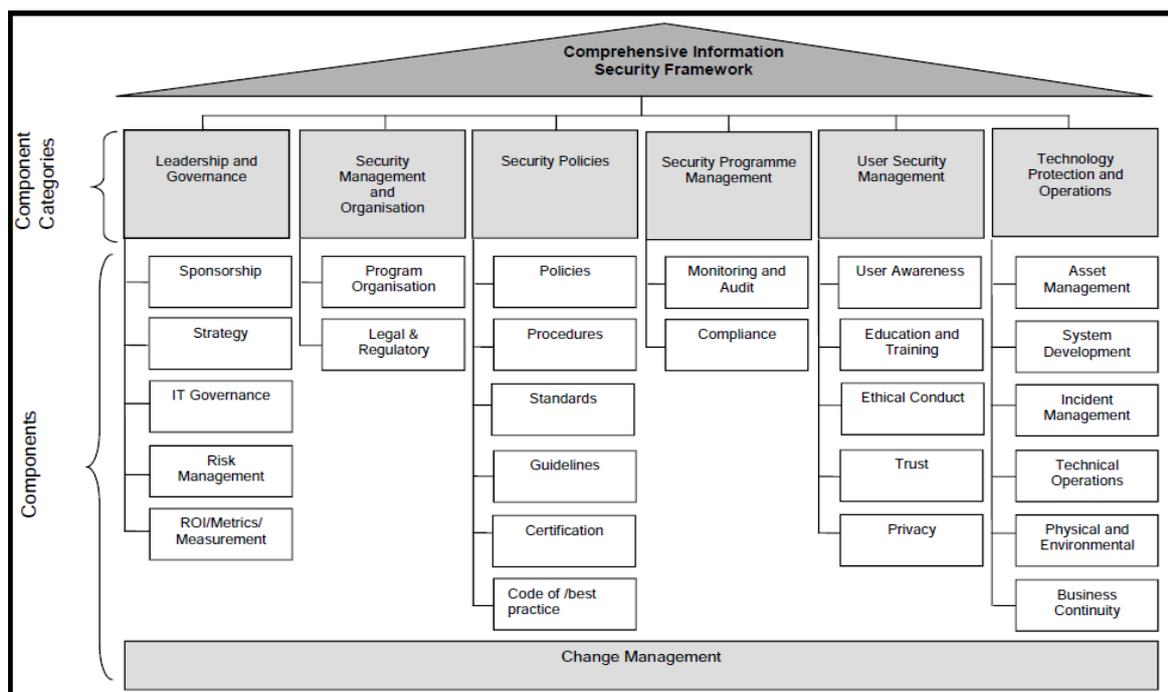
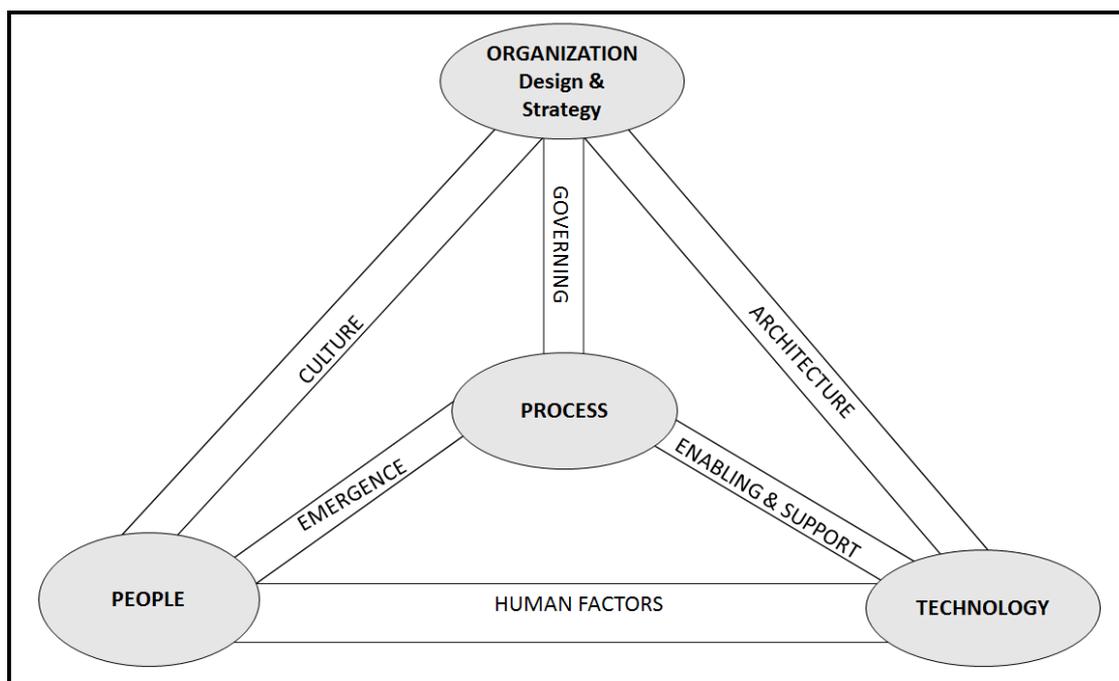


Figure 1: The Comprehensive Information Security Framework (Da Veiga, 2008)

The CISF is a broad framework that can be used in different types of environments. This is the reason it has been identified and used in this research study. As depicted in the diagram,

the CISF is structured in six component categories. The categories are leadership and governance, security management and organisation, security policies, security programme management, user security management, and technology protection and operations.

The CISF contains components that can be used to formulate the proposed model in this research article. The components that have been identified as building blocks are leadership and governance, policies, code of best practice, user awareness, and compliance. Figure 2 depicts the Business Model for Information Security.

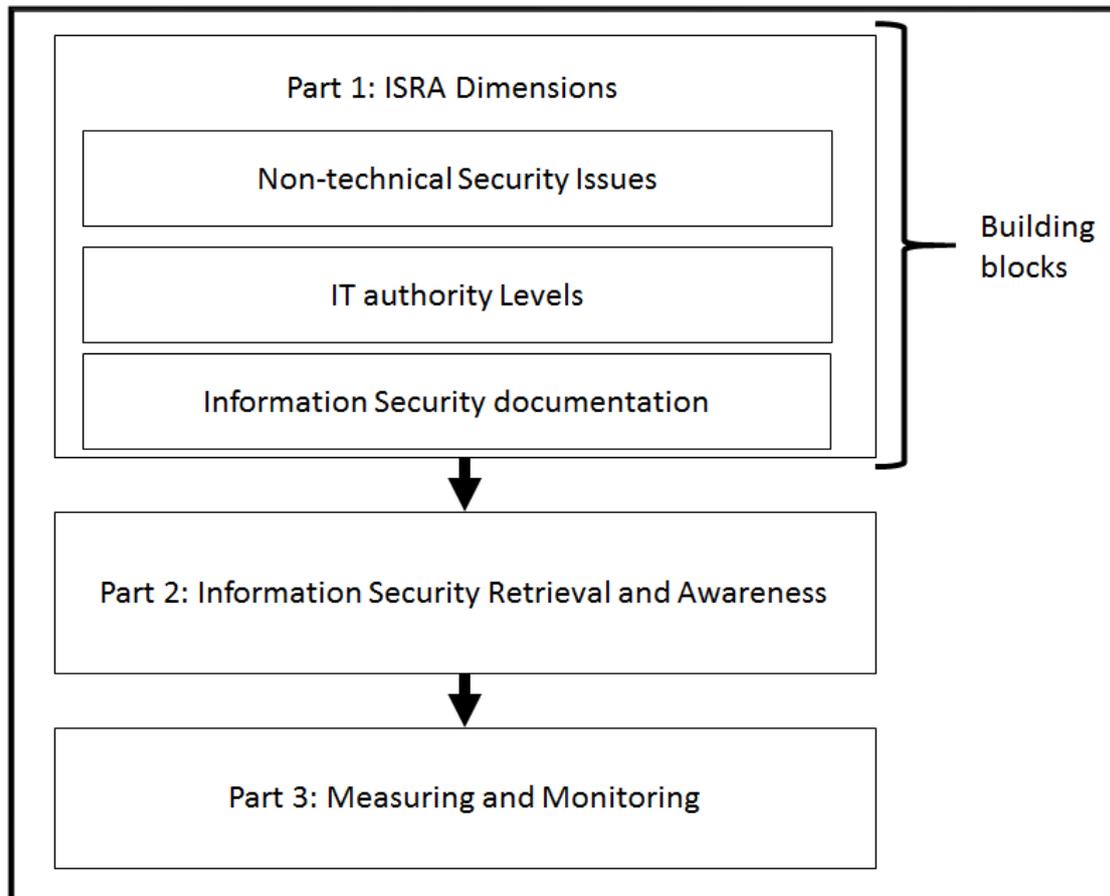


*Figure 2: The Business Model for Information Security (ISACA, 2009)*

According to ISACA (ISACA, 2009), the Business Model for Information Security takes the business-oriented approach to managing information security. It is further stated that the model can be used in any type of enterprise no matter the size of that organisation, it is technology independent, and is applicable across industries, geographies and governing laws.

This model consists of components that are closely related to the topic of this research article. These components are people, enabling and support, human factors, governing, culture, and technology and they will be used as building blocks during the formulation of

the proposed model in this research article. The fact that the model can be used in any type of enterprise is of vital importance and can be useful to this research study. Figure 3 depicts the Information Security Retrieval and Awareness (ISRA) model.



*Figure 3: The Information Security Retrieval and Awareness (ISRA) (Kritzinger, 2006)*

According to Kritzinger (Kritzinger, 2006) the main aim of the ISRA model is to enhance the information security awareness of employees of an organisation. As depicted in figure 3, Kritzinger (Kritzinger, 2006) states that the ISRA model consists of three main parts, namely the ISRA dimensions, information security retrieval and awareness, and measuring and monitoring. The building blocks that have been identified from the ISRA model are information security documentation and measuring and monitoring. These components are important in the South African context and will be used in the formulation of the proposed framework. This model will assist with the enhancement of information security awareness in South African education.

### **ICT models in education**

This subsection discusses ICT models in education that exist in literature. These models will also be used as the building blocks for the proposed model. Figure 4 depicts the Four In Balance model. Draper (Draper, 2010) proposes the use of the Four In Balance Model, which states that the use of ICT in education requires four basic elements, namely vision, expertise, digital learning materials and ICT infrastructure. ICT adds value to the teaching and learning methods when these four (Four In Balance) elements are in balance (Draper, 2010).

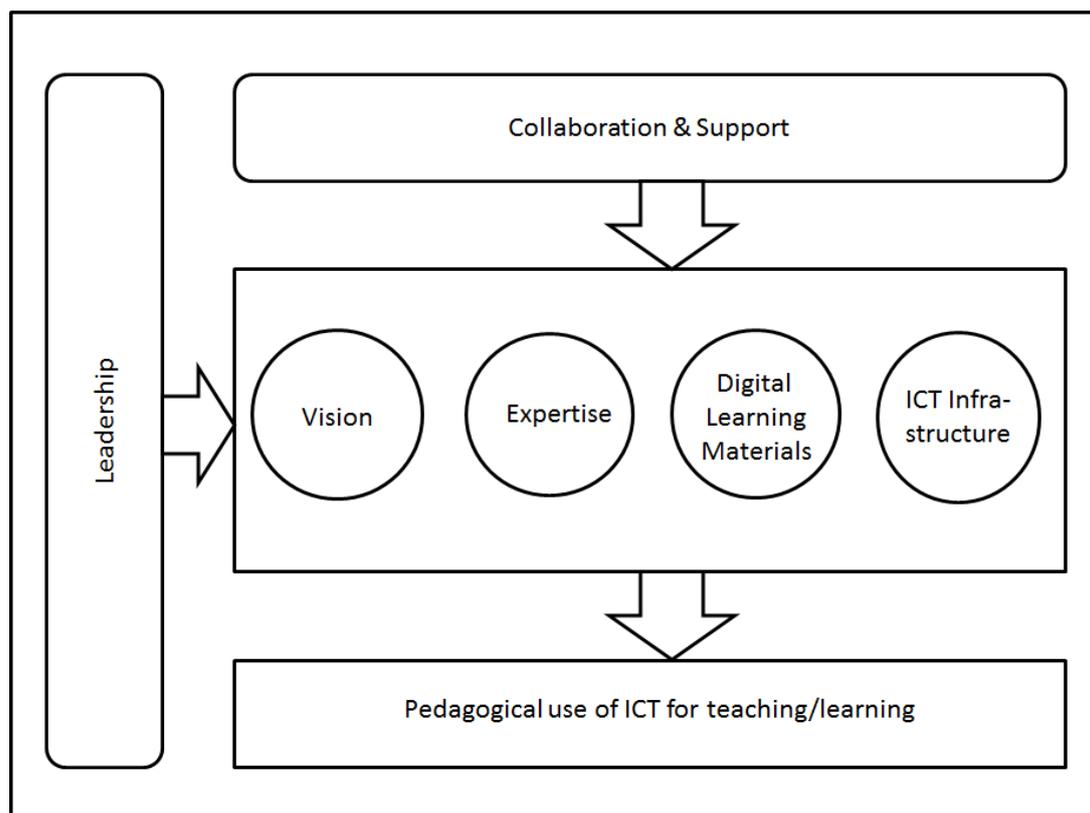
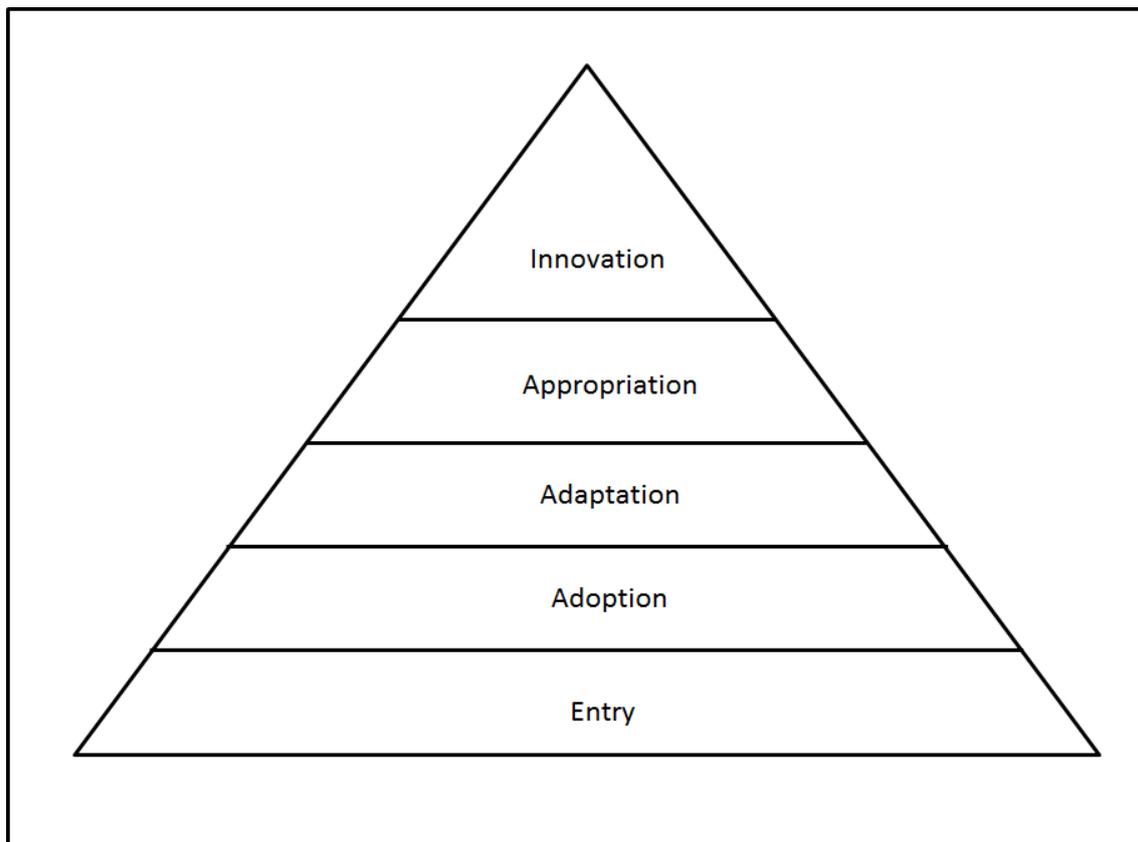


Figure 4: The Four In Balance Model (Draper, 2010)

Of the four aspects presented in this model, Draper (Draper, 2010) mentions that expertise is of utmost importance. The model reveals that teacher expertise is the skills and knowledge required for the usage of ICT (Draper, 2010). Collaboration and support, leadership, and digital learning materials can be used as building blocks when constructing the framework for this research article. The collaboration and support component will be used to bridge the gap that has been identified between the two spheres.

The Department of Education (Department of Education, 2007) and Ndlovu and Lawrence (Ndlovu and Lawrence, 2012) suggest the Teacher Development Framework for the training

and the development of educators in ICT. This framework comprises the various levels such as entry, adoption, adaptation, appropriation and innovation.

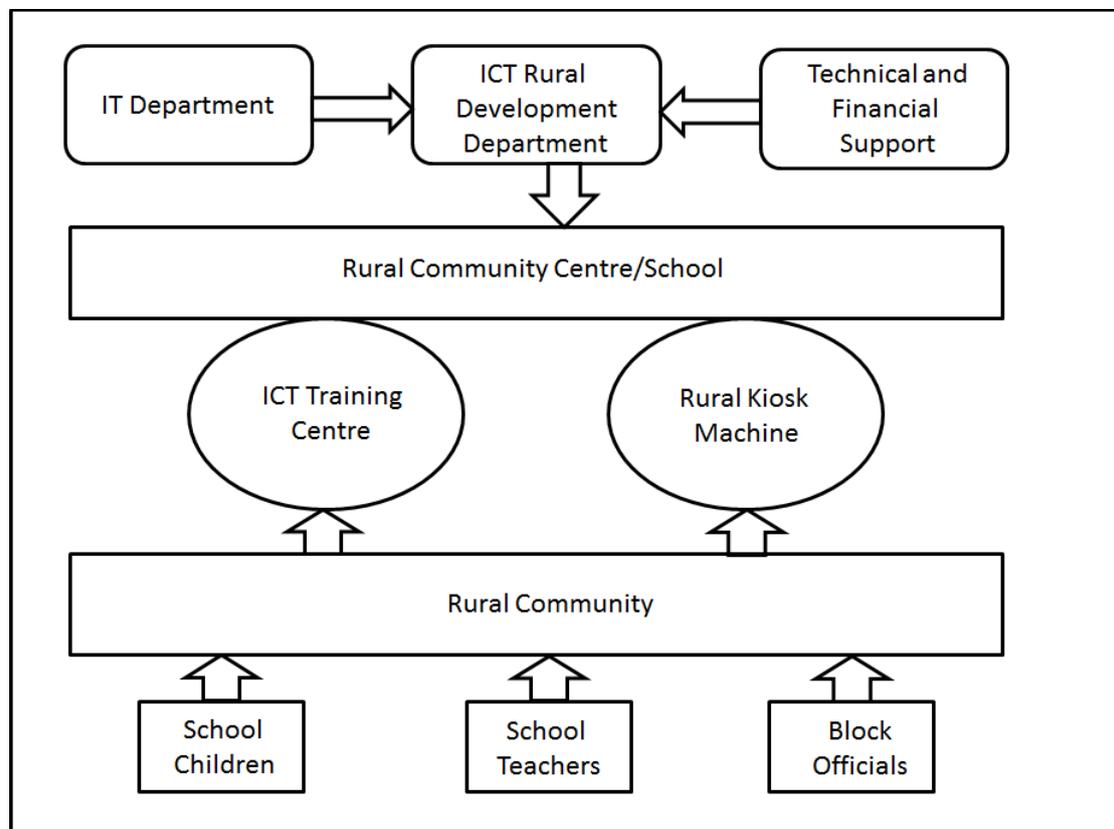


*Figure 5: The Teacher Development Framework (Department of Education, 2007)*

At the entry level of the framework, the Department of Education (Department of Education, 2007) states that educators should acquire the basic skills and knowledge of ICT; at the adoption and adaptation levels of the framework, the educators should acquire the integrative ICT knowledge and skills; and at the appropriation and innovation levels of the framework, the educators should acquire the specialised ICT knowledge and skills. This framework serves as a guide for educators to gauge the levels of ICT skills and knowledge they need to acquire for the usage of ICT in education.

The building block that has been identified from this framework is innovation, and it will also be used in the formulation of the proposed framework of this research article. This framework is important because it is aimed at teachers, and teachers are responsible for the education of school learners.

Roy (Roy, 2012) proposes a model called Model for ICT Rural Education to assist with the integration of ICT in rural schools in India. In this model, Roy (Roy, 2012) proposes a lot of interactions between different stakeholders, which have interest in the development of rural areas in India. The Model for ICT Rural Education is depicted in figure 6.



*Figure 6: Model for ICT Rural Education (Roy, 2012)*

Even though the model looks as if it could be ideal for South African schools, it seems as if it would require extensive financial support (for the establishment and maintenance of the ICT infrastructure). If it were to be implemented in South Africa, it would also require support from the rural communities involved.

One of the main components of this model is school children, which are also one of the main focus areas of this research article. Some of the other building blocks from this model are ICT training centre, community and technical and financial support.

## **THE PROPOSED FRAMEWORK**

This section is divided into four parts. The first part consists of the models and frameworks that were discussed in section 4, the second part discusses the various building blocks that have been identified, the third part consists of the gap analysis, and the fourth part consists of the findings of this research article. The finding also proposes a new and integrated framework that will assist with the integration of ICT security awareness into the South African schooling system.

### **Models and frameworks**

As discussed in section 4, various ICT security and education models and frameworks have been identified in literature. These models and frameworks are as follows:

- A = The Information Security retrieval and Awareness (ISRA) model
- B = The Business Model For Information Security
- C = The Comprehensive Information Security Framework (CISF)
- D = The Teacher Development Framework
- E = The Four In Balance Model
- F = The Model for ICT Rural Education

Each of the models and frameworks mentioned above contains important building blocks that will be used to formulate the proposed framework of this research article. These identified building blocks are discussed in section 5.2.

### **The building blocks**

The different building blocks as identified in section 4 are as follows:

#### **Leadership and governance**

The Department of Communications (DoC) and Independent Communications Authority of South Africa (ICASA) are the main custodians of ICT in South Africa. Therefore, it is their responsibility to ensure the level of ICT security awareness among school learners. These institutions need to play a more vocal and visible role in improving and enhancing the level of ICT security awareness in the country.

It is also in these institutions' best interest to ensure that there is sufficient ICT security awareness among South African citizens. These institutions must play a leadership role in ensuring ICT security and also ensure that there is awareness among the citizens, especially the young people of South Africa. These institutions must delegate and come up with ways to govern the usage of ICT in the country and they need to come up with ways to ensure there is sufficient ICT security awareness.

### **User awareness**

With the South African school learners being some of the top users of technology in the country (MyBroadband, 2014), it is imperative that they are equipped with as much ICT security knowledge as possible. The increase of cyber-crime in the country and the stories that have been published in the media (Belayneh, no date) have shown that there is a need for increased ICT security awareness in the country.

The cyber-crime that has occurred in recent years in South Africa mostly took place in banking institutions and sadly these institutions have refused to take responsibility for these crimes (Belayneh, no date). Given the vulnerabilities of children in South Africa and the amount of crime in the country, it is of utmost importance that school learners are made aware of ICT security. Children in the country face many risks such as human trafficking, rape, cyber-bullying and many more. It is, therefore, very important to ensure that the level of security awareness among school learners is high.

### **Information security documentation**

The main custodians of ICT in South Africa and the tertiary institutions need to create databases, libraries and information stores where information security documentation can be kept and made available to all citizens of the country. This will assist those who are able and willing to learn more about information security in South Africa.

The information security documentation should be made available to all South African school learners. The more information security documentation is available, the better for everyone in the ICT industry and country at large.

### **Policies and standards**

There are many policies and standards that govern the usage of ICT in the world and it has been proven time and again that any institution, organisation and/or country that implements effective policies and standards will be successful. Researchers and government institutions spend lots of money and resources to formulate good policies and standards so that they can be successful.

In South Africa it is the responsibility of the Department of Communications and ICASA to ensure that there are sufficient and effective policies and standards in place. These policies and standards can eliminate and/or reduce the risks posed by ICT among school learners. Tertiary institutions can play a major role in assisting the government to formulate these policies and standards that are relevant to South African school learners.

### **Code of best practice**

An effective code of best practice document should be formulated for use by all South African school learners who make use of ICT. This code of best practice documentation should be communicated and enforced on all school learners in the country. It should also be explained to the school learners that the code of best practice is for their benefit and is for the betterment of the country (like fighting crime).

### **Human factors**

There are many factors that contribute to the lack of ICT security awareness in South Africa. Some of these factors are issues such as culture and people's attitude towards technology. In some instances, issues like ignorance play a major role in people's ICT security awareness.

The human factor is a big issue when it comes to ICT security awareness in developing countries like South Africa. Factors such as low levels of or inadequate education in developing countries are a major problem.

### **Collaboration and support**

Tertiary institutions (like the University of South Africa – UNISA), government institutions (like the State Information Technology Agency – SITA), schools and other stakeholders (such as the Information Security South Africa – ISSA) need to collaborate with each other to formulate collaboration and support structures that all school learners in South Africa can

use to learn about ICT security and the dangers of ICT. This collaboration can also be used for the dissemination of ICT security awareness information to South African school learners.

The South African government should establish and set up a hotline to support victims of ICT-related crimes in South Africa. For instance, if someone has encountered cyber-crime, they should be able to call a toll-free number where they will be assisted and advised on the necessary steps to take. The government should set up and employ an ombudsman to deal specifically with the complaints and victims of ICT-related crime in South Africa. This will assist in reducing the number of ICT-related crime incidents in the country.

### **ICT training and learning centres**

The government of South Africa needs to set up adequate ICT training and learning centres around the country to educate school learners about ICT security. One classroom in all schools should be set up as a training and learning centre where school learners will be taught about ICT-related crime during their early schooling years.

### **Measuring and monitoring**

South African schools need to have mechanisms in place to measure and monitor the usage of ICT and ICT security awareness. The South African government should also ensure that they do a thorough measurement and monitoring of the usage of ICT and ICT security awareness in South African schools.

The gullibility of school learners necessitates the need for constant monitoring and measuring of their ICT usage to ensure that they use it responsibly. Guidelines and rules should be written for all school learners who use ICT and they should be encouraged to abide by them at all times.

Without compromising the privacy of the school learners, it is necessary that the measuring and monitoring controls are put in place in order to overcome the problem of the lack of ICT security awareness in the country. The South African government needs to take responsibility and put these measuring and monitoring controls in place and ensure that they are communicated to school learners across the country.

**Innovation**

The ICT security stakeholders in South Africa need to come up with ideas for the innovation of new ways to fight the problem of ICT-related crime. It is evident that the perpetrators of ICT-related crimes in South Africa are frequently coming up with new ways to commit their crimes, which is why it is very important to ensure that there are new ways to combat these crimes.

Government institutions (such as SITA) must organise more seminars like the GovTech to get together ICT professionals, academics and experts from the ICT industry to come up with ideas to combat and assist in reducing the ICT-related crimes in the country. The private sector can also play a role by sponsoring events and competitions where experts can be asked to come up with ideas and new ways to try and combat these ICT-related crimes.

**Incident management**

The government of South Africa must ensure that there are sufficient incident management procedures in place to be used when ICT-related crimes have occurred. A trend has been seen in the past few years when ICT-related crimes in South African banks have occurred. The banks are continuously denying responsibility and acknowledgement; instead they are blaming their clients citing negligence on their side. An incident management plan will go a long way in assisting the victims of ICT-related crimes in South Africa.

**Compliance**

The custodians of ICT in South Africa must make sure that school learners comply with the laws of the country related to ICT usage. In South Africa there is the ECT Act, which is meant to govern the ICT usage in the country. It is the government's responsibility to ensure that the school learners as well as all other institutions in the country comply with the Act.

**School children**

This is one of the most important building blocks of this research article. The school learners are what this research article is focusing on. The integration of ICT security awareness in South African education is the main focus of this research article.

**The gap analysis**

This section presents a table to depict the gap analysis of the various models and frameworks that have been mentioned in section 4. The gap analysis of this research article is depicted in table 1.

*Table 1: The gap analysis*

	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>
<b>Leadership and governance</b>		X	X		X	
<b>User awareness</b>	X		X			
<b>Information security documentation</b>	X		X			
<b>Policies and standards</b>			X			
<b>Code of best practice</b>			X			
<b>Human factors</b>		X				X
<b>Collaboration and support</b>		X			X	X
<b>ICT training and learning centres</b>			X			X
<b>Measuring and monitoring</b>	X		X			
<b>Innovation and technology</b>		X		X		
<b>Incident management</b>	X		X			
<b>Compliance</b>			X			
<b>School children</b>		X				X

In table 1, the building blocks that were identified and discussed in section 4 are listed in the first column. Columns A, B and C represent the ICT security models and frameworks and columns D, E and F represent the ICT in education models and frameworks.

As depicted in table 1, there is a notable gap between the ICT security models and frameworks and the ICT in education models and frameworks. At the moment it seems the ICT security models and frameworks do not include ICT in education. The framework that is proposed in this research article will integrate the ICT security models and frameworks with the ICT in education models and frameworks. Figure 7 depicts the current situation formulated from the gap analysis that was done in table 1.



*Figure 7: Gap analysis results*

Figure 7 depicts the results that were formulated from the gap analysis done in table 1. The proposed framework is depicted and discussed in section 5.4.

### **Findings**

The framework proposed in this research article bridges the gap that is identified in section 5.3 and integrates the ICT security models and frameworks with the ICT in education models and frameworks. The purpose of this exercise is to formulate a framework that is inclusive of both sides and one that is relevant to the South African context. Figure 8 depicts the proposed framework.

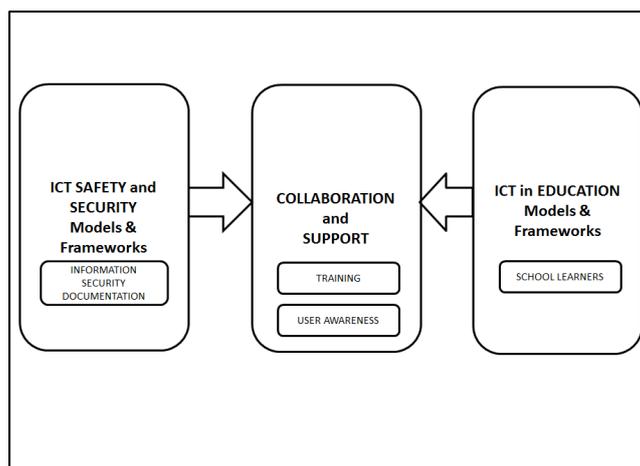


Figure 8: The proposed framework

The proposed framework in figure 8 integrates the ICT security models and frameworks with the ICT in education models and frameworks resulting in an all-inclusive framework that is relevant to both parties involved. From the gap analysis results that were shown in figure 7, a new component is added. This component will facilitate the integration between the two spheres. Figure 9 depicts the newly introduced component – collaboration and support – which contains all the identified building blocks in a flowing sequence.

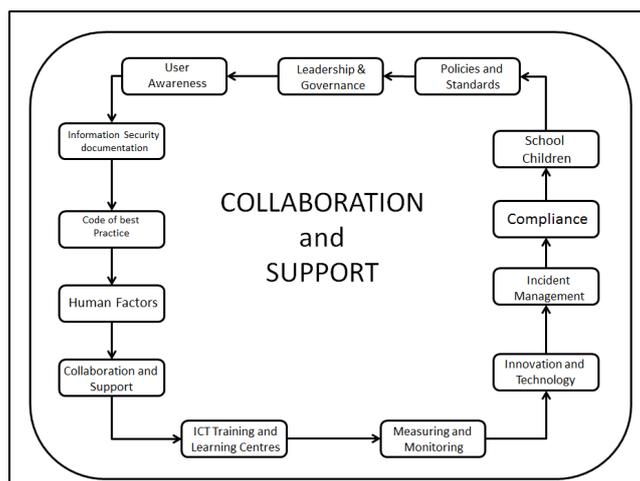


Figure 9: The collaboration and support component

Figure 9 focuses on the newly proposed component called collaboration and support. This component comprises of all the building blocks that were identified and discussed in section 5.2. The building blocks in figure 9 are shown in a flowing sequence because they are all related to each other. The conclusions of this research article are discussed in section 6.

## **CONCLUSION**

Even though there are models and frameworks related to ICT security in literature, there is still a gap when it comes to models and frameworks that are specifically directed towards South African school learners. This article proposed a framework to integrate ICT security awareness into the South African schooling system.

The literature review that was conducted clearly showed that the models and frameworks that are existent in literature do not cater for the challenges that are faced by South African school learners. This means that the South African school learners are at a risk and are vulnerable to ICT-related crimes. The literature review also made the author aware of the high number of ICT-related crimes in South Africa. This necessitates the need to educate and inform, not only the school learners, but also the general population at large about the dangers posed by the usage of ICT.

The research study has allowed the researcher to propose a framework that is specific to South African school learners in the plight to fight against ICT-related crimes. It has proposed a framework to assist to integrate ICT security awareness into the South African schooling system. The researcher proposed, among other ideas, the setting up of an ombudsman office for ICT-related crime in South Africa. This will be beneficial especially towards the victims of ICT-related crimes.

For future research, one can look at drafting policies and procedures that would be used by the proposed ombudsman for ICT-related crimes in the country. Also, one can look at the curriculum that would be taught at the proposed ICT training and learning centres. Another aspect that can be looked at is the formulation of the code of best practice document that will be used by all ICT stakeholders in South Africa.

## **REFERENCES**

Adedayo, W. S. and Ayobami, A. S. (2013) 'Relationship between information security

awareness and information security threat', *INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT*, 3, pp. 115–119. Available at:

<http://ssrn.com/abstract=2328542>.

Ahmad, A. (2012) 'Type of Security Threats and It's Prevention.', *International Journal of Computer Technology & Applications*, 3(2), pp. 750–752. Available at:

<http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Type+of+Security+Threats+and+It's+Prevention#0> (Accessed: 13 January 2015).

Alnatheer, M. and Nelson, K. (2009) 'Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context', in *Proceedings of the 7th Australian Information Security Management Conference*. Security Research Institute Conferences.

Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=ism>.

Aloul, F. A. (2012) 'The Need for Effective Information Security Awareness', *Journal of Advances in Information Technology*, 3(3), pp. 176–183. doi: 10.4304/jait.3.3.176-183.

Alper, Y. A. (2011) 'Controlling Insider Threats With Information Security Policies', in *ECIS 2011 Proceedings*, pp. 1–12.

Amedzo, K. E. (2007) *The Integration of Information and Communication technology into Rural Schools of South Africa: A Case Study of Schools in Malamulele*. Stellenbosch University. Available at: <http://scholar.sun.ac.za/handle/10019.1/2135>.

Andress, J. (2011) *The Basics of Information Security: Understanding the fundamentals of InfoSec in theory and practice*. Edited by Russ Rogers. Waltham: Syngress Press.

Ashraf, S. (2005) 'Organization Need and Everyone's Responsibility Information Security Awareness', *The SANS Institute - Global Information Assurance Certification Paper*, (Security 401).

Beckers, K., Heisel, M. and Hatebur, D. (2009) 'Supporting Common Criteria Security Analysis with Problem Frames\*', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(300266902), pp. 37–63.

Belayneh, B. (no date) *South African Centre for Information Security*. Available at:

<http://www.sacfis.co.za/index.htm> (Accessed: 14 June 2014).

Bell ICT Solutions (2007) *The Benefits of ICT*. Available at:

---

<http://www.bell.ca/web/enterprise/newsRoom/en/pdf/Benefits-of-ICT-White-Paper-EN.pdf>.

Brownson, S. (2014) 'Student Experiential Learning of Cyber Security through Virtualization', *Journal of Research in Innovative Teaching*, 7(1), pp. 112–118.

Bushati, J. *et al.* (2012) 'Advantages and Disadvantages of Using ICT in Education', in *International Conference in Europe*, pp. 1–17. Available at:

<http://bederweb.majdanov.net/Conferences/ICES 2012/FULL>

ARTICLE/Bushati\_Barolli\_Dibra\_Haveri\_Advantages and disadvantages of using ICT in education.pdf.

Chetty, J. and Coetzee, M. (2010) 'Towards an information security framework for service-oriented architecture', in *Information Security for South Africa*. IEEE, pp. 1–8. doi: 10.1109/ISSA.2010.5588272.

Chi, M. (2011) 'Security Policy and Social Media Use'. The SANS Institute. Available at: <http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749>.

Chigona, A. and Chigona, W. (2010) 'An Investigation Of Factors Affecting The Use Of ICT For Teaching In The Western Cape Schools', in *18th European Conference on Information Systems*, p. 12.

Communications Security Establishment Canada (2013) 'Cyber Security Risks of Using Social Media Guidance for the Government of Canada', pp. 1–2.

Creswell, J. W. (2009) *Research Design: Qualitative, Quantitative and Mixed Approaches (3rd Edition)*, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. doi: 10.2307/1523157.

Department of Communications (2010) 'The South African Cyber Security Policy', *Government Gazette*, pp. 1–16. doi: <http://dx.doi.org/9771682584003-32963>.

Department of Communications (2014) 'National Integrated ICT Policy Green Paper', *Government Gazette*, 24 January, pp. 3–104. Available at: [www.gpwonline.co.za](http://www.gpwonline.co.za).

Department of Education (2004) 'White Paper on e-Education'. *Government Gazette*, pp. 3–46. Available at:

---

<http://www.education.gov.za/LinkClick.aspx?fileticket=Keu0%2FBkee%2BM%3D&tabid=191&mid=484>.

Department of Education (2007) 'Guidelines for Teacher Training and Professional Development in ICT'.

Dlamini, Z. and Modise, M. (2012) 'Cyber Security Awareness Initiatives in South Africa: A Synergy Approach', in *7th International Conference on Information Warfare and Security*. Seattle, USA: Academic Conferences International, pp. 62–83. doi: 10.1007/978-3-8349-4134-3\_3.

Dlodlo, N. (2009) 'Access to ICT education for girls and women in rural South Africa: A case study', *Technology in Society*. Pretoria, 31(2), pp. 168–175. doi: doi:10.1016/j.techsoc.2009.03.003.

Draper, K. (2010) *Understanding science teachers' use and integration of ICT in a developing country context*. University of Pretoria. Available at: <http://upetd.up.ac.za/thesis/available/etd-02032011-132142/unrestricted/thesis.pdf>.

Drevin, L., Kruger, H. A. and Steyn, T. (2007) 'Value-focused assessment of ICT security awareness in an academic environment', *Computers & Security*, 26(1), pp. 36–43. doi: 10.1016/j.cose.2006.10.006.

Edwards, C. K. (2013) *A Framework for the Governance of Information Security, Computers & Security*. Nova Southeastern University. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404804002639> (Accessed: 26 January 2015).

Fibikova, L. and Mueller, R. (2012) 'Threats, Risks and the Derived Information Security Strategy', in *Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference (2012)*. Daimler Northeast Asia Ltd, pp. 11–20. doi: 10.1007/978-3-658-00333-3\_2.

Ford, M. and Botha, A. (2010) 'A Pragmatic Framework for Integrating ICT into Education in South Africa', in Paul Cunningham and Miriam Cunningham (ed.) *IST-Africa 2010 Conference Proceedings*. Port Elizabeth: IIMC International Information Management Corporation, pp. 1–10.

- Fourie, L. and McNamara (2008) *Enhancing the Livelihoods of the Rural Poor Through ICT: A Knowledge Map, South Africa Country Study*. 13. Available at: [http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037\\_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf](http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf).
- Francis, L.-A. (2010) *DOC prioritises cyber security*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=34338:doc-prioritises-cyber-security](http://www.itweb.co.za/index.php?option=com_content&view=article&id=34338:doc-prioritises-cyber-security) (Accessed: 14 June 2014).
- Fu, J. S. (2013) 'ICT in Education : A Critical Literature Review and Its Implications', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 9(1), pp. 112–125.
- Gillwald, A., Moyo, M. and Stork, C. (2012) 'What is happening in ICT in South Africa: A supply-and demand-side analysis of the ICT sector', *Evidence for ICT Policy Action*. Research ICT Africa, (7). Available at: <http://www.researchictafrica.net/docs/Policy Paper 7 - Understanding what is happening in ICT in South Africa.pdf>.
- Gokhe, M. (2000) 'Concept of Information, Communication and Educational Technology', *Thakur Shyamnarayan College of Education and Research (TSCER)*, p. 81. Available at: [http://www.tscermumbai.in/resources\\_paper\\_4/IV.1\\_information\\_and\\_communication\\_technology.pdf](http://www.tscermumbai.in/resources_paper_4/IV.1_information_and_communication_technology.pdf).
- Government of the Hong Kong Special Administrative Region (2008) *An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region*. Hong Kong. Available at: <http://www.infosec.gov.hk/english/technical/files/overview.pdf>.
- Grobler, M., Vuuren, J. J. Van and Leenen, L. (2012) 'Implementation of a Cyber Security Policy in South Africa : Reflection on Progress and the Way Forward Current State of Cyber Security Research in South Africa', in *ICT Critical Infrastructures and Society*. Amsterdam: Springer Berlin Heidelberg, pp. 215–225. doi: 10.1007/978-3-642-33332-3\_20.
- Grobler, M., Vuuren, J. J. Van and Zaaiman, J. (2011) 'Evaluating Cyber Security Awareness in South Africa', *10th European Conference on Information Warfare and Security ECIW-2011*, pp. 113–121.

Gundemeda, N. (2014) 'Information Technology (IT) Education in Andhra Pradesh: A Sociological View', *Journal of Social Sciences*, 40(3), pp. 333–342. Available at: [http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemeda-N/JSS-40-3-333-14-1567-Gundemeda-N-Tx\[5\].pdf](http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemeda-N/JSS-40-3-333-14-1567-Gundemeda-N-Tx[5].pdf) (Accessed: 2 October 2014).

Gundu, T. and Flowerday, S. V (2013) 'Ignorance to Awareness: Towards an Information Security Awareness Process', *SAIEE Africa Research Journal*, 104(2), pp. 69–79.

Hancock, B., Ockleford, E. and Windridge, K. (2009) 'An Introduction to Qualitative Research', *The NIHR RDS EM/YH*. Available at: <http://books.google.cz/books?id=sFv1oWX2DoEC>.

Higgins, S. (2003) 'Does ICT Improve Learning and Teaching in Schools?', *Journal of Science and Technology*. Bera, 17(6), pp. 586–594. Available at: <http://www.bera.ac.uk/files/reviews/ict-pur-mb-r-f-p-1aug03.pdf>.

Hong, K. S. and Songan, P. (2011) 'ICT in the changing landscape of higher education in Southeast Asia', *Australasian Journal of Educational Technology*, 27(8), pp. 1276–1290. doi: 10.14742/ajet.893.

Information Security Resource Center (no date) *Basic Information Security Principles*. Available at: [http://www.oregon.gov/DAS/CIO/ISRC/pages/intro\\_basics.aspx](http://www.oregon.gov/DAS/CIO/ISRC/pages/intro_basics.aspx).

Internet Service Provider's Association (no date) *419 Scams*. Available at: <http://ispa.org.za/spam/419-scams/>.

ISACA (2009) *An Introduction to the Business Model for Information Security*. ISACA. Available at: <http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>.

Isisag, K. U. (2012) 'The Positive Effects of Integrating ICT in Foreign Language Teaching', in *ICT for Language Learning*. Available at: [http://conference.pixel-online.net/ICT4LL2012/common/download/Paper\\_pdf/235-IBT107-FP-Isisag-ICT2012.pdf](http://conference.pixel-online.net/ICT4LL2012/common/download/Paper_pdf/235-IBT107-FP-Isisag-ICT2012.pdf).

Jabareen, Y. (2009) 'Building a conceptual framework: philosophy, definitions, and procedure', *International Journal of Qualitative Methods*, 8, pp. 49–62. doi: 10.2522/ptj.20100192.

John, V. (2015) *Education MEC promises to take Gauteng classrooms into the future*,

- Mail&Guardian*. Available at: <http://mg.co.za/article/2015-05-20-education-mec-promises-to-take-gauteng-classrooms-into-the-future> (Accessed: 27 August 2015).
- Johnson, M. (2012) 'Cybercrime: Threats and Solutions', Available at SSRN. Ark Group. Available at: <http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf> (Accessed: 13 January 2015).
- Kabay, M. E. (2002) 'What's Important for Information Security: A Manager's Guide'. Northfield: Norwich University, pp. 1–4.
- Kayle, A. (2011) *SA's security awareness lags*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=42395](http://www.itweb.co.za/index.php?option=com_content&view=article&id=42395).
- Kortjan, N. and Von Solms, R. (2014) 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal*, 52, pp. 29–41. Available at: <http://sacj.cs.uct.ac.za/index.php/sacj/article/view/201/95>.
- Kreutzer, T. (2009) 'Assessing Cell Phone Usage in a South African Township School', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*. Cape Town: e/merge, 5(5), pp. 43–57. Available at: <http://emerge2008.net>.
- Kritzinger, E. (2006) *An Information Security Retrieval And Awareness Model For Industry*. University of South Africa. Available at: <http://uir.unisa.ac.za/bitstream/handle/10500/2475/thesis.pdf?sequence=1>.
- Kritzinger, E. and Padayachee, K. (2007) 'Teaching Safe and Secure usage of ICTs in South African Schools', in *Proceedings of the 2nd International Conference on Society and Information Technologies*. Pretoria, pp. 1–6. Available at: <http://hdl.handle.net/10500/3986>.
- Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security*. Elsevier Ltd, 29(8), pp. 840–847. doi: 10.1016/j.cose.2010.08.001.
- Kruger, H. A., Drevin, L. and Steyn, T. (2006) 'A Framework For Evaluating ICT Security Awareness', in *Information Security for South Africa*, pp. 1–11.
- Kruger, H. a. and Kearney, W. D. (2008) 'Consensus ranking – An ICT security awareness case study', *Computers & Security*. Elsevier Ltd, 27(7–8), pp. 254–259. doi:

---

10.1016/j.cose.2008.07.001.

Kyobe, M. (2010) 'Towards a framework to guide compliance with IS security policies and regulations in a university', in *Information Security for South Africa*. Ieee, pp. 1–6. doi: 10.1109/ISSA.2010.5588651.

Kyobe, M. E., Molai, P. and Salie, T. (2009) 'Investigating electronic records management and compliance with regulatory requirements in a South African university', *SA Journal of Information Management*, 11(1), pp. 1–15. doi: 10.4102/sajim.v11i1.396.

De Lange, M. and Von Solms, R. (2013) 'An e - Safety Educational Framework in South Africa', in *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Cape Town, p. 497. Available at: [http://www.satnac.org.za/proceedings/2012/papers/3.Internet\\_Services\\_End\\_User\\_Applications/53.pdf](http://www.satnac.org.za/proceedings/2012/papers/3.Internet_Services_End_User_Applications/53.pdf).

Lau, K. and Albion, P. R. (2010) 'Hong Kong Home Economics Teachers' Adoption of ICT for Learning and Teaching', in Romeo, G. and Gronn, D. (eds) *Digital Diversity Australian Computers in Education Conference 2010*. ACCE. Available at: <http://eprints.usq.edu.au/7354/>.

Liu, Z., Shu, G. and Lee, D. (2011) *Network Security, Administration and Management*. Edited by D. C. Kar and M. R. Syed. IGI Global. doi: 10.4018/978-1-60960-777-7.

Maholwana-Sotashe, N. L. (2007) *Challenges faced by secondary school teachers in integrating ICT into the curriculum: A multiple case study in the Grahamstown Circuit*. Rhodes University.

Mdlongwa, T. (2012) 'Information and Communication Technology ( ICT ) as a Means of Enhancing Education in Schools in South Africa : Challenges , Benefits and Recommendations'. Pretoria: Africa Institute of South Africa, pp. 1–8.

Mikre, F. (2011) 'The Roles of Information Communication Technologies in Education Review Article with Emphasis to the Computer and Internet', *Ethiopian Journal of Education and Sciences*, 6(2). Available at: <http://www.ajol.info/index.php/ejesc/article/view/73521/62437>.

Miller, L., Naidoo, M. and Belle, J. Van (2003) 'Critical Success Factors for ICT Interventions in

---

Western Cape Schools'. Cape Town: Department of Information Systems, University of Cape Town, pp. 1–14.

Minister of Justice and Correctional Services (2017) *Cybercrimes and Cybersecurity Bill*. Republic of South Africa. doi: -.

Moll, I. *et al.* (2007) 'Status Report on ICTs and Higher Education in South Africa'. Braamfontein: South African Institute for Distance Education (SAIDE). Available at: [http://www.judybackhouse.com/pdfs/saide\\_status\\_of\\_elearning\\_in\\_sa.pdf](http://www.judybackhouse.com/pdfs/saide_status_of_elearning_in_sa.pdf).

Mullamaa, K. (2010) 'ICT in Language Learning--Benefits and Methodological Implications', *International Education Studies*, 3(1), pp. 38–44. Available at: <http://www.ccsenet.org/journal/index.php/ies/article/view/4965/4131>.

MyBroadband (2014) *SA students pour R6.1 billion into tech*. Available at: <http://businesstech.co.za/news/general/55685/sa-students-pour-r6-1-billion-into-tech/>.

Mzekandaba, S. (2015) *Cybercrime cost SA over R3.42bn in 2013*, *ITWeb Africa*. Available at: <http://www.itwebafrica.com/security/514-south-africa/234087-cybercrime-cost-sa-over-r342bn-in-2013> (Accessed: 15 March 2015).

Ndlovu, N. S. and Lawrence, D. (2012) 'The quality of ICT use in South African classrooms', in *Towards Carnegie III*. Cape Town: University of Cape Town.

Nevondwe, L. and Odeku, K. O. (2014) 'Protecting Children from Exposure to Pornography in South Africa', *Bangladesh e-Journal of Sociology*, 11(2), pp. 132–142.

Ngcobo, M. (2009) 'A strategic promotion of language use in multilingual South Africa: information and communication', *Southern African Linguistics and Applied Language Studies*, 27(1), pp. 113–120. doi: 10.2989/SALALS.2009.27.1.9.757.

Nyakowa, S. L. (2014) *Factors Influencing ICT Adoption Among Public Secondary School Teachers : A Case of Webuye Sub-County, Bungoma County, Kenya*. University of Nairobi.

Oates, B. J. (2011) *Researching Information Systems and Computing*. London: Sage Publications Ltd.

Olivier, M. S. (2004) *Information Technology Research: A practical guide for Computer Science and Informatics*. 2nd edn. Pretoria: Van Schaik Publishers.

Ope, J. (2014) *An Information Systems Security Framework for Kenyan Public Universities*.

- University of Nairobi. Available at: <http://erepository.uonbi.ac.ke/handle/11295/76933> (Accessed: 20 January 2015).
- Plessis, A. and Webb, P. (2012) 'A Teacher Proposed Heuristic For ICT Professional Teacher Development and Implementation In The South African Context', *Turkish Online Journal of Educational Technology*, 11(4), pp. 46–55.
- Poepjes, R. and Lane, M. (2012) 'An Information Security Awareness Capability Model (ISACM )', in *Australian Information Security Management Conference*. Edith Cowan University Research Online. Available at: <http://ro.ecu.edu.au/ism/137>.
- PriceWaterhouseCoopers (2010) *Information and Communication Technology for Education in India and South Asia, ICT in School Education (Primary and Secondary)*. Available at: [http://www.infodev.org/infodev-files/resource/InfodevDocuments\\_1016.pdf](http://www.infodev.org/infodev-files/resource/InfodevDocuments_1016.pdf).
- Qureshi, I. A., Whitty, M. and Whitty, M. (2014) 'Facebook as e-learning tool for higher education institutes', *Knowledge Management & E-Learning*, 6(4), pp. 440–448.
- Radovanovic, D., Radojević, T. and Sarac, M. (2010) 'IT audit in accordance with Cobit standard', in *MIPRO, 2010 Proceedings of the 33rd International Convention*. Opatija, Croatia: IEEE Xplore, pp. 1137–1141. Available at: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5533627](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5533627).
- Romm, N. R. A. and Phil, D. L. (2013) 'Employing Questionnaires in terms of a Constructivist Epistemological Stance: Reconsidering Researchers' Involvement in the Unfolding of Social Life', *International Journal of Qualitative Methods*, pp. 652–669.
- Rotich, D. C. and Munge, E. M. (2007) 'An overview of electronic information resources sharing initiatives in Kenyan universities', *SA Jnl Libs & Info Sci*, 73(1), pp. 64–74.
- Rowe, D. C., Lunt, B. M. and Ekstrom, J. J. (2011) 'The role of cyber-security in information technology education', *Proceedings of the 2011 conference on Information technology education - SIGITE '11*. New York, New York, USA: ACM Press, 2, p. 113. doi: 10.1145/2047594.2047628.
- Roy, A. et al. (2014) 'Promoting proper education for sustainability: An exploratory study of ICT enhanced Problem Based Learning in a developing country', *International Journal of Education and Development using Information and Communication Technology*, 10(1), pp.

70–90.

Roy, N. K. (2012) 'ICT-Enabled Rural Education in India', *International Journal of Information and Education Technology*, 2(5), pp. 525–529. doi: 10.7763/IJJET.2012.V2.196.

Saleh, Z. I., Heba, R. and Mashhour, A. (2011) 'Proposed Framework for Security Risk Assessment', *Journal of Information Security*, 02(02), pp. 85–90. doi: 10.4236/jis.2011.22008.

Saunders, M., Lewis, P. and Thornhill, A. (2008) *Research Methods for Business Students*, *Research methods for business students*. doi: 10.1007/s13398-014-0173-7.2.

Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students*. Pearson Education Limited.

Smit, D. (2015) 'Cyberbullying in South African and American schools: A legal comparative study', *South African Journal of Education*, 35(2), pp. 1–11. doi: 10.15700/saje.v35n2a1076.

Smith, E. H. and Kruger, H. A. (2010) 'A framework for evaluating IT security investments in a banking environment', in *Information Security for South Africa*. Sandton: IEEE, pp. 1–7. doi: 10.1109/ISSA.2010.5588343.

Von Solms, S. and Von Solms, R. (2014) 'Towards Cyber Safety Education in Primary Schools in Africa', in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, pp. 185–197.

Straker, L. *et al.* (2010) 'Evidence-based guidelines for the wise use of computers by children: physical development guidelines.', *Ergonomics*, 53(4), pp. 458–77. doi: 10.1080/00140130903556344.

Straker, L., Pollock, C. and Maslen, B. (2009) 'Principles for the wise use of computers by children.', *Ergonomics*, 52(11), pp. 1386–401. doi: 10.1080/00140130903067789.

Surty, M. E. (2011) 'Quality education for rural schools in South Africa – challenges and solutions', *South African Rural Educator*. South Africa: Department of Basic Education, pp. 8–15.

Swanepoel, A. J. (2015) *Towards A Framework For Understanding Information Systems*. University of Pretoria. doi: 2263/50796.

The European Network and Information Security Agency (ENISA) (2010) *The new users'*

---

*guide: How to raise information security awareness*. Available at:

[http://www.enisa.europa.eu/publications/archive/copy\\_of\\_new-users-guide](http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide).

UNESCO (2012) 'Why Language Matters for the Millenium Development Goals', in *Language, Education and the Millennium Development Goals*. Bangkok: UNESCO Bangkok.

UNICEF (2012) 'South African mobile generation. Study on South African young people on mobiles', pp. 1–47. doi:

[http://www.unicef.org/southafrica/SAF\\_resources\\_mobilegeneration.pdf](http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf).

Da Veiga, A. (2008) *Cultivating and Assessing Information Security Culture*. University of Pretoria. doi: <http://hdl.handle.net/2263/24117>.

Venktes, K. (2016) *SA falls in key global ICT index, fintech24*. Available at:

<http://www.fin24.com/Tech/News/sa-falls-in-key-global-ict-index-20161122> (Accessed: 15 May 2017).

Veríssimo, P. and Rodrigues, L. (2001) 'Fundamental Security Concepts', in *Distributed Systems for System Architects*. Springer US, pp. 377–393. doi: 10.1007/978-1-4615-1663-7\_16.

Vermeulen, J. (2014a) *Critical security bug gets SA sites, hosts scrambling, mybroadband*.

Available at: <http://mybroadband.co.za/news/security/100324-critical-security-bug-gets-sa-sites-hosts-scrambling.html>.

Vermeulen, J. (2014b) *New online banking fraud scheme in South Africa, mybroadband*.

Available at: <http://mybroadband.co.za/news/general/100368-new-online-banking-fraud-scheme-in-south-africa.html>.

Walaza, M., Loock, M. and Kritzinger, E. (2014) 'A Framework to Integrate ICT Security Awareness into the South African Schooling System', in *SAICSIT '14 Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology*. Pretoria: ACM, p. 11. doi: 10.1145/2664591.2664596.

Walaza, M., Loock, M. and Kritzinger, E. (2015) 'A Pragmatic Approach towards the Integration of ICT Security Awareness into the South African Education System', in *The Second International Conference on Information Security and Cyber Forensics (InfoSec2015)*.

Cape Town, pp. 35–40.

Wayman, I. and Kyobe, M. (2012) 'Incorporating Knowledge of Legal and Ethical Aspects into Computing Curricula of South African Universities', *Journal of Information Technology Education: Innovations in Practice*, 11.

Whitman, M. E. and Mattford, H. J. (2011) *Road Map To Information Security: For IT And InfoSec Managers*. Boston: Course Technology.

## Appendix B: Accepted Research Article – ISTE2015

### TOWARDS A FRAMEWORK FOR INTEGRATING ICT SECURITY AWARENESS WITH SOUTH AFRICAN EDUCATION

<b>Mvelo Walaza</b>	<b>Marianne Loock</b>	<b>Elmarie Kritzinger</b>
<b>University of South Africa</b>	<b>University of South Africa</b>	<b>University of South Africa</b>
<b>South Africa</b>	<b>South Africa</b>	<b>South Africa</b>
<a href="mailto:53315804@mylife.unisa.ac.za">53315804@mylife.unisa.ac.za</a>	<a href="mailto:loockm@unisa.ac.za">loockm@unisa.ac.za</a>	<a href="mailto:kritze@unisa.ac.za">kritze@unisa.ac.za</a>

**ABSTRACT**– Information and Communication Technology (ICT) security in South Africa is classified as an important component of national security. The framework proposed in this article was created based on a number of models and frameworks from various research studies conducted around the world. The building blocks used to construct the proposed framework were specifically chosen to establish a framework that would be relevant to South Africa. This research article considered all building blocks that were included in the proposed framework, as well as the various components and sub-components of the proposed framework. Having included the components (Information Repositories, Language, ICT Security Curriculum, and ICT Security Ombudsman) that were identified to be missing from the gap analysis, the ICT Security Awareness Framework for Education (ISAFE) was proposed and discussed in detail. Lastly, the results of the literature review analysis were reported and the proposed framework was clearly depicted.

**Keywords:** ICT, education, models, frameworks, security, awareness.

## **1. INTRODUCTION**

The level of Information and Communication Technology (ICT) usage among school learners in South Africa is rising at a rapid rate (MyBroadband, 2014). This high volume of ICT usage necessitates the need for introducing security measures among local school learners. Given the general consensus on the importance of ICT security, this research study investigated the possibility of integrating it with the South African education system.

Having traced a number of existing models and frameworks related to ICT security and education in available literature, the researcher reviewed and analyzed them and came to the conclusion that a gap exists between them. He also found that the existing frameworks and models were not necessarily relevant in the South African context. The gap analysis and literature review that were conducted in respect of the existing models and frameworks encouraged this research to propose the ICT Security Awareness Framework for Education (ISAFE), as it was believed that this framework would be more relevant and suitable for South African conditions.

An in-depth literature review was conducted in section 3, where the new components of the ISAFE were discussed. However, the main aim of the current article was to discuss the detail of the ISAFE and explain its relevance to the South African context. The findings of this research were discussed and explained, future research was proposed, and lastly, the conclusions drawn from the research were discussed.

## **2. RESEARCH METHODOLOGY**

### **2.1 Background**

This section investigated the problem statement, research questions and research objectives, as well as the research methodology used in this research. First, the problem statement was attended to in Section 2.2.

### **2.2 Problem Statement**

In order to ensure that the proposed framework was relevant to South Africa, a number of components were added to the framework. The need for these added components formed the basis of the problem statement:

- No framework exists to assist with the integration of ICT security awareness into the South African education system.

The problem statement as formulated above aimed to address the components that would make the framework more appropriate for the South African environment.

### **2.3. Research questions, objectives and deliverables**

The research question as formulated for this study was:

- What components can be added to the existing framework to ensure that it is relevant to the South African schooling environment?

The aim of the above research question was to find a solution to the unsuitability of the proposed framework to the South African schooling environment and has led the author to propose the following research objective:

- To propose and investigate components that do not exist in the proposed framework and that are relevant to the South African schooling environment, and to depict the entire proposed framework.

The intended deliverable was to provide a breakdown of the proposed framework and give a brief explanation of each of the components including the added components.

### **2.4. Methodology**

An in-depth literature review was conducted to become au fait with past scholarly work. Reliable sources such as the [businesstech.co.za](http://businesstech.co.za) website (MyBroadband, 2014) were also used to gather information about the South African ICT security situation.

Each of the main components of the proposed framework was depicted and discussed thoroughly. Once the main components had been discussed, the sub-components within them were described and discussed, followed by an overview of the sub-components. Lastly, the entire proposed framework was depicted, showing all components and sub-components.

### **3. LITERATURE REVIEW**

This section covered the literature review that was carried out for this study.

#### **3.1. ICT Security in South African Education**

In recent years, the number of internet users and Internet Service Providers (ISP) in South Africa has grown exponentially (Kritzinger and Padayachee, 2007). Various interventions were made, such as the South African government's introduction of the National Cyber Security Policy (Department of Communications, 2010; Grobler, Vuuren and Leenen 2012), but these interventions still do not guarantee the ICT security of school learners.

South African school learners are generally vulnerable to ICT-related crime. The serious extent to which school learners can be vulnerable to ICT-related crime has prompted Walaza, Looek and Kritzinger (2014) and Kritzinger and Padayachee (2007) to propose the inclusion of ICT security awareness initiatives in the South African school curriculum.

#### **3.2. ICT Security Awareness Models and Frameworks in South Africa**

During their research, Walaza *et al* (2014) used a number of models and frameworks from their literature review to conduct a gap analysis and construct the proposed framework. Two of these – the Information Security Retrieval and Awareness (ISRA) model and the Teacher Development Framework – are from research studies done in South Africa. Kyobe (2010) also proposed a framework for guiding compliance with information system security policies and regulations in a university.

The frameworks and models in South African literature are focused not only on academia, but are also focused on the private sector as well. For instance, Smith and Kruger (2010) proposed a framework for evaluating information technology security investments in a banking environment. Local research studies that evaluate ICT security awareness in South Africa as a whole were discussed in section 3.3.

#### **3.3. ICT Security Awareness in South Africa**

The usage of ICT across various industries has caused a rise in knowledge economy which is essential for negotiating with the global societies (Gundimeda 2014). According to Dlamini and Modise (2012) South Africa is one of the top three countries that have been targeted for phishing attacks. This has caused some institutions to embark on initiatives to empower South African citizens. The CEO of the South African Centre for Information Security (SACfIS), Mr. Beza Belayneh, raised a number of concerns when it comes to ICT-related crime in South Africa in the last couple of years. Some of these incidents include the stealing of R50 million worth of airtime from MTN by some East European nationals, a huge amount of money stolen from an Absa account belonging to the CEO of Media24 (Belayneh, no date).

The South African government has played its role by introducing the Electronic Communications and Transactions Act, 25 of 2002 (ECT Act) and the National Cyber Security Policy with the aim of protecting its citizens against cybercrime (Department of Communications, 2010). This proves that there is sufficient information and policies available about ICT security awareness in South Africa – the problem is adherence to and the implementation of these policies.

#### 4. BACKGROUND TO THE RESEARCH STUDY

Table 1 presents the gap analysis that was done to compare the ICT security models and frameworks with ICT models and frameworks in education.

*Table 1. The gap analysis (Walaza et al, 2014)*

	<b>A The Information Security Retrieval and Awareness (ISRA) model</b>	<b>B The Business Model For Information Security</b>	<b>C The Comprehensive Information Security Framework (CISF)</b>	<b>D The Teacher Development Framework</b>	<b>E The Four- In- Balance Model</b>	<b>F The Model for ICT Rural Education</b>
<b>Leadership and governance</b>		X	X		X	
<b>User awareness</b>	X		X			
<b>Information security documentation</b>	X		X			
<b>Policies</b>			X			

<b>and standards</b>						
<b>Code of best practice</b>			X			
<b>Human factors</b>		X				X
<b>Collaboration and support</b>		X			X	X
<b>ICT training and learning centres</b>			X			X
<b>Measuring and monitoring</b>	X		X			
<b>Innovation and technology</b>		X		X		
<b>Incident management</b>	X		X			
<b>Compliance</b>			X			
<b>School children</b>		X				X

In Table 1, the building blocks that were identified by Walaza *et al* (2014) were listed in bold in the left-most column of the table. The different models and frameworks from which the building blocks were derived were listed in bold on the first row of Table 1 and were also marked as A, B, C, D, E and F. The letter “X” was used to identify the building blocks that exist in more than one model or framework. As can be seen from Table 1, more building blocks were encountered in the ICT security models and frameworks than in the ICT in education models and frameworks. This observation has allowed the researcher to conclude that there is indeed a gap between the two spheres. Hence, a framework was suggested to incorporate ICT security awareness into the South African schooling system.

In addition to the components that had been derived from the various models and frameworks, the researcher proposed the addition of specific components to ensure that the proposed framework was relevant to the South African context. Section 4.1 next gives a detailed overview of the added components.

#### **4.1. An overview of the added components**

In the framework that was proposed by Walaza *et al* (2014) it was suggested that certain components had to be introduced to ensure that the proposed framework would be relevant to the South African schooling environment. The components that were added are Language, ICT Security Ombudsman, ICT Security Curriculum, and Information Repositories.

The components were added in order to attempt to bridge the gap (identified during the gap analysis) between the two spheres, namely; ICT security and ICT in education. It was also an attempt to make the proposed framework more relevant to South Africa.

#### **4.2. Language**

According to Ngcobo (2009), South Africa has been commended for its multilingual language policy, but the implementation of the policy is still a problem. This research study proposed that the dissemination of all information pertaining to ICT security awareness be done in indigenous languages.

Roy *et al* (2014) stated that many ICT-related software applications are built with the incorrect assumption that it is easy for school learners to understand non-native languages. UNESCO (2012) also emphasised the importance of using native languages in learning by documenting that better results have been achieved when learners learn through medium of their native languages. The points mentioned in the research performed by Roy *et al* (2014) and UNESCO (2012) confirmed the importance of using native languages when trying to promote ICT security awareness among school learners.

#### **4.3. ICT Security Ombudsman**

The establishment of an ICT security ombudsman office was a notion that was proposed by this research study. The literature review has revealed that such an office does not exist in South Africa. However, since a vast number of ICT-related crimes have occurred in recent years in the country (Belayneh, no date), such an office would be very beneficial to South Africa. Walaza *et al* (2014) referred to the high crime rate in South Africa and stressed the need for proper ICT security measures to be put in place.

The office of the South African ICT security ombudsman will perform similar duties as other ombudsman offices such as the insurance ombudsman, the tax ombudsman and the banking ombudsman. In the event that a person has been a victim of ICT-related crime, would like to lay a complaint, or is struggling to get compensation from a service provider; then the victim will have a dedicated office that can be contacted.

#### **4.4. ICT Security Curriculum**

Chigona and Chigona (2010) and other scholars such as Ford and Botha (2010) stated that even though there have been attempts to equip schools and educators with ICT skills for curriculum inclusion and delivery in South Africa, there is still evidence of the low adoption of ICT among educators in schools. Hence, the current research article proposed that an ICT security curriculum be included in the general South African school curriculum.

Research studies that have been conducted (Kritzinger & Padayachee, 2007; Wayman & Kyobe, 2012) have shown that ICT security awareness has been insufficiently incorporated into the South African school curriculum. Wayman and Kyobe (2012) emphasised the importance of the inclusion of ICT security in school curricula. They stated that during their research (surveys and interviews), the participants showed a lack of knowledge of critical legislation. This re-emphasized the need for the inclusion of ICT security awareness in the school curricula.

#### **4.5. Information Repositories**

This research study proposed that the South African government must set up information repositories that store information about ICT security. These repositories will be used for information sharing and must be accessed easily and freely by all school learners in South Africa.

The information repositories will comprise ICT security-related research papers, websites, social networks, magazine articles, newspaper articles and research articles in electronic as well as print format. The repositories will take the form of mobile kiosks and will be placed in relevant areas such as police stations, libraries, hospitals, municipal offices and community halls.

### **5. THE PROPOSED FRAMEWORK**

The proposed framework was named the ICT Security Awareness Framework for Education (ISAFE). This section presented the different phases of the proposed framework.

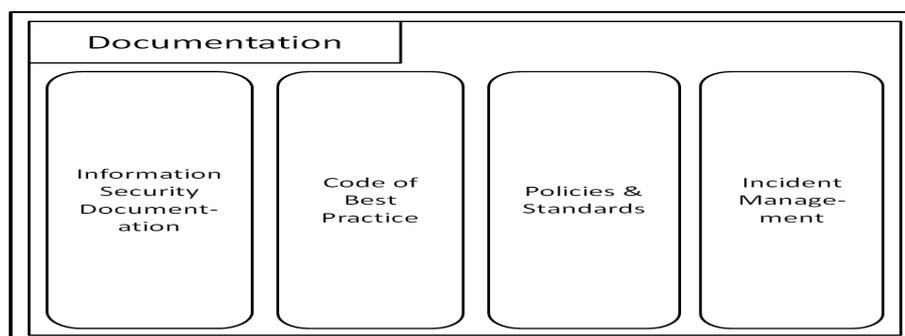
#### **5.1. The Leadership & Governance component**

The Leadership & Governance component was derived from the Comprehensive Information Security Framework (CISF) (Da Veiga, 2008). The South African government will

have to play a leadership and governing role when it comes to the integration of ICT security awareness in South Africa's education system.

## 5.2. The Documentation component

The Documentation component was derived from the ISRA (Kritzinger, 2006) model. This building block will be used for all the documentation that is relevant to ICT security awareness in South African schools. Within this component are sub-components that depict the ICT security documentation in literature which will be used to ensure the effective integration of the education and security awareness spheres. Figure 1 depicts the components within the Documentation sub-component.



**Fig. 1. The Documentation component**

The sub-components within the Documentation component – Information Security Documentation, Code of Best Practice, Policies & Standards, and Incident Management – were discussed briefly in the paragraphs below.

**Information Security Documentation:** This sub-component was derived from the ISRA model and it involves all the documentation related to information security. This is the documentation that will be made available to South African school learners in order to enhance their ICT security awareness.

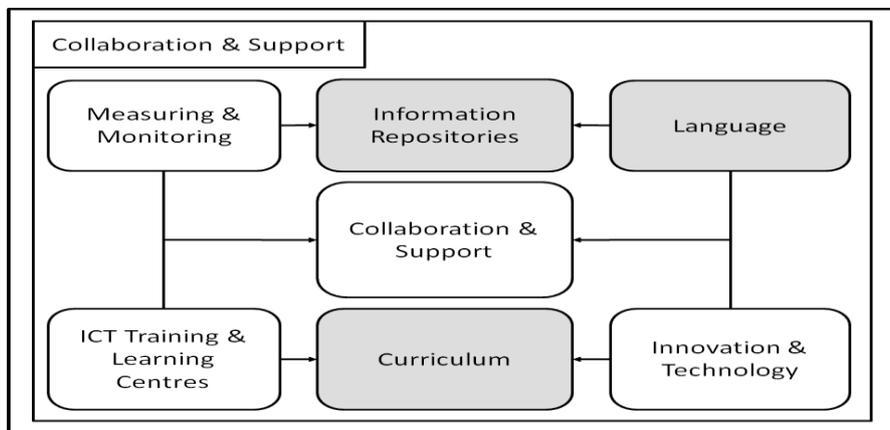
**Code of Best Practice:** This sub-component was derived from the CISF. This component investigates the code of best of practice for ICT security in South Africa and will encourage school learners to read and adhere to these practices.

**Policies and Standards:** This sub-component was derived from the CISF and it involves the best policies and standards that must be adhered to by school learners in South Africa. The latter will be encouraged to follow and adhere to the policies and standards that govern the usage of ICT at all times.

**Incident Management:** This sub-component was taken from the CISF framework. This component will be responsible for the documentation of all incident management procedures that must be followed by school learners.

**5.3. The Collaboration & Support component**

This component was derived from the Four-In-Balance Model. In the present research study, the collaboration & support component will be accountable for integrating the two spheres (ICT security models and ICT in education models). This component contains a number of sub-components that are used to ensure the integration of ICT security awareness in South African schools. Figure 2 depicts the Collaboration & Support component of the proposed ISAFE.



**Fig. 2. The Collaboration & Support component**

The four sub-components of the Collaboration & Support component are Measuring & Support, Collaboration & Support, ICT Training & Learning Centres, and Innovation & Technology. The researcher earlier introduced additional ICT components to make the proposed framework more relevant to South Africa (inter alia Information Repositories, Language, Curriculum) and these were discussed in section 4.1. The remaining components are discussed in the upcoming paragraphs.

**Measuring & Monitoring:** This sub-component, which was derived from the ISRA model, is responsible for measuring and monitoring ICT security awareness among school learners in South Africa.

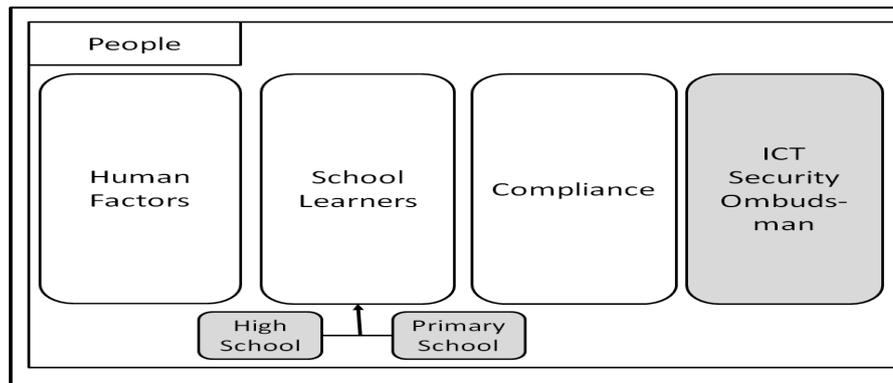
**Collaboration & Support:** This sub-component was derived from the Four-In-Balance Model. In the present research this component will be used to facilitate collaboration in respect of the dispensing of ICT security information among education institutions in South Africa.

**ICT Training & Learning Centres:** This sub-component was derived from the Model for ICT Rural Education (Roy, 2012). The current study proposes the establishment of training and learning centres to assist with introducing ICT security awareness among school learners.

**Innovation & Technology:** This sub-component was derived from both the Teacher Development Framework (Department of Education, 2007) and the Business Model for Information Security (ISACA, 2009). Technology in the form of mobile phones, mobile apps and websites will be utilized to enhance and integrate ICT security awareness in South African schools.

#### **5.4. The People component**

This component was derived from the Business Model for Information Security (ISACA, 2009). It is responsible for all the human aspects of this study. The proposed new sub-component, ICT Security Ombudsman, will also be depicted here. The sub-components of the People component of the proposed ISAFE are illustrated in Figure 3 below.



**Fig. 3. The People Component**

The initial sub-components within the People component were Human Factors, School Learners and Compliance. The ICT Security Ombudsman was discussed earlier (in Section 4.1) as one of the new components that were included in the ISAFE. The School Learners component introduces two sub-components called High School and Primary School. These and the rest of the components were discussed in the following paragraphs.

**Human Factors.** This sub-component was derived from the Business Model for Information Security (ISACA, 2009). This component will investigate some of the human factors that might influence ICT security awareness among South African school learners.

**School Learners.** The School Learners sub-component, which is one of the main components of the current research study, was derived from the Model for ICT Rural Education (Roy, 2012). The researcher proposed the addition of two sub-components called High School and Primary School to this component, so as to make a distinction between the two types of school learners. Caution must be exercised in respect of the type of information made available to high school and primary school learners.

**Compliance.** This sub-component was derived from the CISF. It investigates policy compliance among ICT stakeholders in South Africa, specifically among school learners.

### **5.5. The User Awareness component**

The User Awareness component was derived from the CISF. It is responsible for all the ICT security awareness programmes and initiatives that will be directed towards the South African school learners.

## 6. THE ICT SECURITY AWARENESS FRAMEWORK FOR EDUCATION

The whole ISAFE, showing all the components and their sub-components, was depicted in

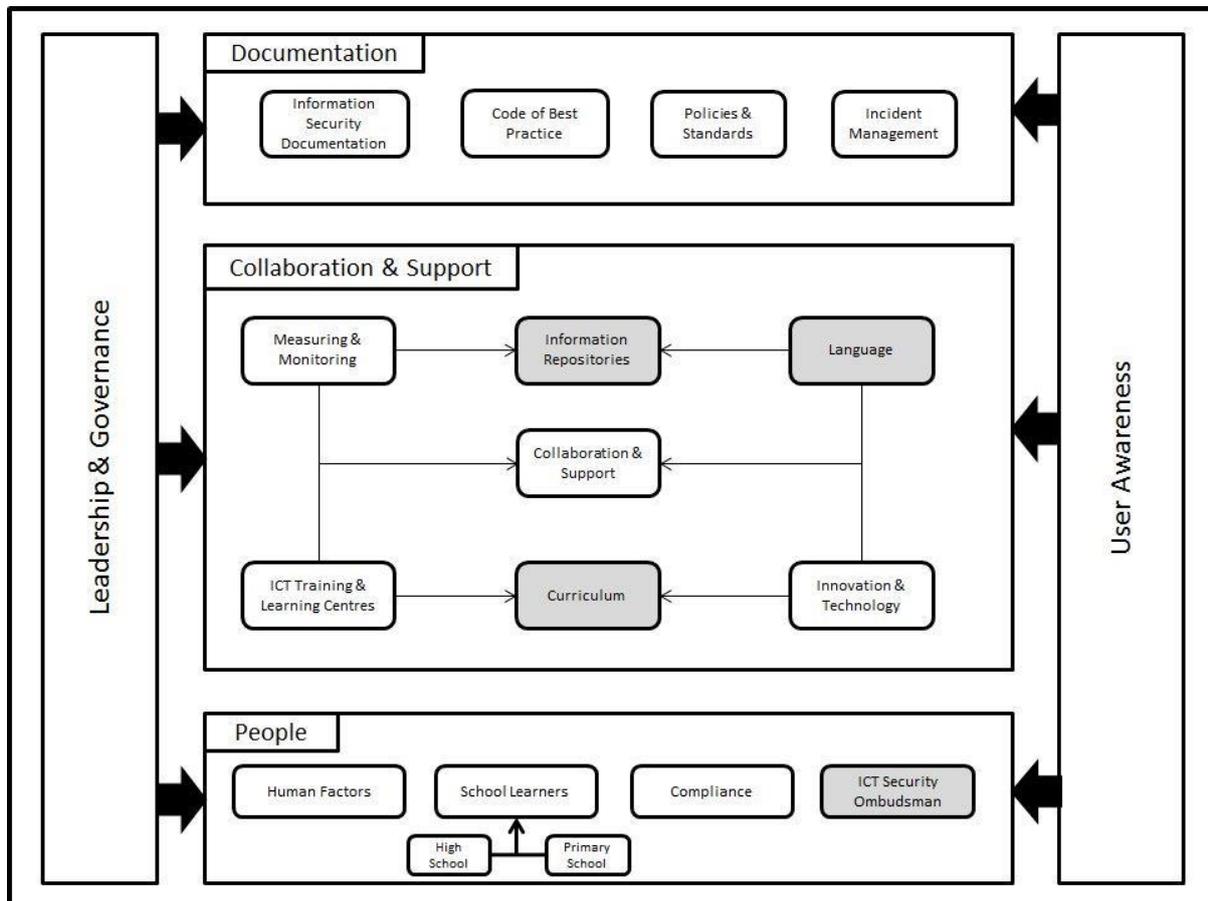


Figure 4.

Figure 4: ICT Security Awareness Framework for Education (ISAFE)

The sub-components that have been newly proposed were coloured grey in the framework so as to distinguish them, from those building blocks in Table 1 that were derived from existing models and frameworks.

As indicated earlier, the main purpose of the ISAFE was the integration of ICT security awareness in South African education. The literature review conducted by the researcher indicated that the existing models and frameworks were not adequately relevant to South Africa. Hence a new framework that would be more applicable to South Africa had to be proposed.

## **7. FINDINGS**

A notable gap between ICT security models and frameworks on the one hand and the ICT in education models and frameworks on the other has been discovered. The review revealed that there was a need for an ICT security framework that is relevant to South Africa. A comparison was done by drawing up a gap analysis table showing both the ICT security frameworks and the ICT in education frameworks. The gap that was identified between these two spheres was depicted in Table 1, and hence the researcher proposed an adjusted and more relevant framework for South Africa.

The proposed framework, called the ISAFE, attempted to bridge the gap that was identified in this research study and the researcher was of the belief that it was far more relevant in the South African context. The ISAFE is made up of five main components that were discussed in Section 5. These components were identified as building blocks during the literature review and they contain specific sub-components that were more descriptive. Four new components that were not part of the initial building blocks have been included in this proposed framework and were discussed in Section 4.1.

## **8. CONCLUSION**

This article presented an in-depth discussion of the ISAFE. New components, namely Language, ICT Security Ombudsman, ICT Security Curriculum, and Information Repositories were discussed and were believed to make the proposed framework (ISAFE) more relevant to the South African environment. In Section 2 the researcher explained the research methodology, while the problem statement, the research question, research objectives, and research deliverables were subsequently discussed in separate subsections. In Section 3 the literature review that had been conducted for this research was depicted; and this was followed by the background to the research study in Section 4. The different spheres of the proposed framework were reviewed in Section 5, and this was followed by the proposed framework in Section 6; while the findings of the research were discussed in Section 7.

## **REFERENCES**

Adedayo, W. S. and Ayobami, A. S. (2013) 'Relationship between information security awareness and information security threat', *INTERNATIONAL JOURNAL OF RESEARCH IN*

---

COMMERCE, IT & MANAGEMENT, 3, pp. 115–119. Available at:  
<http://ssrn.com/abstract=2328542>.

Ahmad, A. (2012) 'Type of Security Threats and It's Prevention.', *International Journal of Computer Technology & Applications*, 3(2), pp. 750–752. Available at:  
<http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Type+of+Security+Threats+and+It's+Prevention#0> (Accessed: 13 January 2015).

Alnatheer, M. and Nelson, K. (2009) 'Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context', in *Proceedings of the 7th Australian Information Security Management Conference*. Security Research Institute Conferences. Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=ism>.

Aloul, F. A. (2012) 'The Need for Effective Information Security Awareness', *Journal of Advances in Information Technology*, 3(3), pp. 176–183. doi: 10.4304/jait.3.3.176-183.

Alper, Y. A. (2011) 'Controlling Insider Threats With Information Security Policies', in *ECIS 2011 Proceedings*, pp. 1–12.

Amedzo, K. E. (2007) *The Integration of Information and Communication technology into Rural Schools of South Africa: A Case Study of Schools in Malamulele*. Stellenbosch University. Available at: <http://scholar.sun.ac.za/handle/10019.1/2135>.

Andress, J. (2011) *The Basics of Information Security: Understanding the fundamentals of InfoSec in theory and practice*. Edited by Russ Rogers. Waltham: Syngress Press.

Ashraf, S. (2005) 'Organization Need and Everyone's Responsibility Information Security Awareness', *The SANS Institute - Global Information Assurance Certification Paper*, (Security 401).

Beckers, K., Heisel, M. and Hatebur, D. (2009) 'Supporting Common Criteria Security Analysis with Problem Frames\*', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(300266902), pp. 37–63.

Belayneh, B. (no date) *South African Centre for Information Security*. Available at:  
<http://www.sacfis.co.za/index.htm> (Accessed: 14 June 2014).

Bell ICT Solutions (2007) *The Benefits of ICT*. Available at:  
<http://www.bell.ca/web/enterprise/newsRoom/en/pdf/Benefits-of-ICT-White-Paper->

---

EN.pdf.

Brownson, S. (2014) 'Student Experiential Learning of Cyber Security through Virtualization', *Journal of Research in Innovative Teaching*, 7(1), pp. 112–118.

Bushati, J. et al. (2012) 'Advantages and Disadvantages of Using ICT in Education', in *International Conference in Europe*, pp. 1–17. Available at:

<http://bederweb.majdanos.net/Conferences/ICES 2012/FULL>

ARTICLE/Bushati\_Barolli\_Dibra\_Haveri\_Advantages and disadvantages of using ICT in education.pdf.

Chetty, J. and Coetzee, M. (2010) 'Towards an information security framework for service-oriented architecture', in *Information Security for South Africa*. IEEE, pp. 1–8. doi:

10.1109/ISSA.2010.5588272.

Chi, M. (2011) 'Security Policy and Social Media Use'. The SANS Institute. Available at:

<http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749>.

Chigona, A. and Chigona, W. (2010) 'An Investigation Of Factors Affecting The Use Of ICT For Teaching In The Western Cape Schools', in *18th European Conference on Information Systems*, p. 12.

Communications Security Establishment Canada (2013) 'Cyber Security Risks of Using Social Media Guidance for the Government of Canada', pp. 1–2.

Creswell, J. W. (2009) *Research Design: Qualitative, Quantitative and Mixed Approaches (3rd Edition)*, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. doi:

10.2307/1523157.

Department of Communications (2010) 'The South African Cyber Security Policy', *Government Gazette*, pp. 1–16. doi: <http://dx.doi.org/9771682584003-32963>.

Department of Communications (2014) 'National Integrated ICT Policy Green Paper', *Government Gazette*, 24 January, pp. 3–104. Available at: [www.gpwonline.co.za](http://www.gpwonline.co.za).

Department of Education (2004) 'White Paper on e-Education'. *Government Gazette*, pp. 3–46. Available at:

<http://www.education.gov.za/LinkClick.aspx?fileticket=Keu0%2FBkee%2BM%3D&tabid=191>

---

&mid=484.

Department of Education (2007) 'Guidelines for Teacher Training and Professional Development in ICT'.

Dlamini, Z. and Modise, M. (2012) 'Cyber Security Awareness Initiatives in South Africa: A Synergy Approach', in *7th International Conference on Information Warfare and Security*. Seattle, USA: Academic Conferences International, pp. 62–83. doi: 10.1007/978-3-8349-4134-3\_3.

Dlodlo, N. (2009) 'Access to ICT education for girls and women in rural South Africa: A case study', *Technology in Society*. Pretoria, 31(2), pp. 168–175. doi: doi:10.1016/j.techsoc.2009.03.003.

Draper, K. (2010) *Understanding science teachers' use and integration of ICT in a developing country context*. University of Pretoria. Available at: <http://upetd.up.ac.za/thesis/available/etd-02032011-132142/unrestricted/thesis.pdf>.

Drevin, L., Kruger, H. A. and Steyn, T. (2007) 'Value-focused assessment of ICT security awareness in an academic environment', *Computers & Security*, 26(1), pp. 36–43. doi: 10.1016/j.cose.2006.10.006.

Edwards, C. K. (2013) *A Framework for the Governance of Information Security*, *Computers & Security*. Nova Southeastern University. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404804002639> (Accessed: 26 January 2015).

Fibikova, L. and Mueller, R. (2012) 'Threats, Risks and the Derived Information Security Strategy', in *Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference (2012)*. Daimler Northeast Asia Ltd, pp. 11–20. doi: 10.1007/978-3-658-00333-3\_2.

Ford, M. and Botha, A. (2010) 'A Pragmatic Framework for Integrating ICT into Education in South Africa', in Paul Cunningham and Miriam Cunningham (ed.) *IST-Africa 2010 Conference Proceedings*. Port Elizabeth: IIMC International Information Management Corporation, pp. 1–10.

Fourie, L. and McNamara (2008) *Enhancing the Livelihoods of the Rural Poor Through ICT: A*

---

*Knowledge Map, South Africa Country Study*. 13. Available at: [http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037\\_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf](http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf).

Francis, L.-A. (2010) *DOC prioritises cyber security*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=34338:doc-prioritises-cyber-security](http://www.itweb.co.za/index.php?option=com_content&view=article&id=34338:doc-prioritises-cyber-security) (Accessed: 14 June 2014).

Fu, J. S. (2013) 'ICT in Education : A Critical Literature Review and Its Implications', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 9(1), pp. 112–125.

Gillwald, A., Moyo, M. and Stork, C. (2012) 'What is happening in ICT in South Africa: A supply-and demand-side analysis of the ICT sector', *Evidence for ICT Policy Action*. Research ICT Africa, (7). Available at: <http://www.researchictafrica.net/docs/Policy Paper 7 - Understanding what is happening in ICT in South Africa.pdf>.

Gokhe, M. (2000) 'Concept of Information, Communication and Educational Technology', *Thakur Shyamnarayan College of Education and Research (TSCER)*, p. 81. Available at: [http://www.tscermumbai.in/resources\\_paper\\_4/IV.1\\_information\\_and\\_communication\\_technology.pdf](http://www.tscermumbai.in/resources_paper_4/IV.1_information_and_communication_technology.pdf).

Government of the Hong Kong Special Administrative Region (2008) *An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region*. Hong Kong. Available at: <http://www.infosec.gov.hk/english/technical/files/overview.pdf>.

Grobler, M., Vuuren, J. J. Van and Leenen, L. (2012) 'Implementation of a Cyber Security Policy in South Africa : Reflection on Progress and the Way Forward Current State of Cyber Security Research in South Africa', in *ICT Critical Infrastructures and Society*. Amsterdam: Springer Berlin Heidelberg, pp. 215–225. doi: 10.1007/978-3-642-33332-3\_20.

Grobler, M., Vuuren, J. J. Van and Zaaiman, J. (2011) 'Evaluating Cyber Security Awareness in South Africa', *10th European Conference on Information Warfare and Security ECIW-2011*, pp. 113–121.

Gundemeda, N. (2014) 'Information Technology (IT) Education in Andhra Pradesh: A

---

Sociological View', *Journal of Social Sciences*, 40(3), pp. 333–342. Available at: [http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemenda-N/JSS-40-3-333-14-1567-Gundemenda-N-Tx\[5\].pdf](http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemenda-N/JSS-40-3-333-14-1567-Gundemenda-N-Tx[5].pdf) (Accessed: 2 October 2014).

Gundu, T. and Flowerday, S. V (2013) 'Ignorance to Awareness: Towards an Information Security Awareness Process', *SAIEE Africa Research Journal*, 104(2), pp. 69–79.

Hancock, B., Ockleford, E. and Windridge, K. (2009) 'An Introduction to Qualitative Research', *The NIHR RDS EM/YH*. Available at: <http://books.google.cz/books?id=sFv1oWX2DoEC>.

Higgins, S. (2003) 'Does ICT Improve Learning and Teaching in Schools?', *Journal of Science and Technology*. Bera, 17(6), pp. 586–594. Available at: <http://www.bera.ac.uk/files/reviews/ict-pur-mb-r-f-p-1aug03.pdf>.

Hong, K. S. and Songan, P. (2011) 'ICT in the changing landscape of higher education in Southeast Asia', *Australasian Journal of Educational Technology*, 27(8), pp. 1276–1290. doi: 10.14742/ajet.893.

Information Security Resource Center (no date) *Basic Information Security Principles*. Available at: [http://www.oregon.gov/DAS/CIO/ISRC/pages/intro\\_basics.aspx](http://www.oregon.gov/DAS/CIO/ISRC/pages/intro_basics.aspx).

Internet Service Provider's Association (no date) *419 Scams*. Available at: <http://ispa.org.za/spam/419-scams/>.

ISACA (2009) *An Introduction to the Business Model for Information Security*. ISACA. Available at: <http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>.

Isisag, K. U. (2012) 'The Positive Effects of Integrating ICT in Foreign Language Teaching', in *ICT for Language Learning*. Available at: [http://conference.pixel-online.net/ICT4LL2012/common/download/Paper\\_pdf/235-IBT107-FP-Isisag-ICT2012.pdf](http://conference.pixel-online.net/ICT4LL2012/common/download/Paper_pdf/235-IBT107-FP-Isisag-ICT2012.pdf).

Jabareen, Y. (2009) 'Building a conceptual framework: philosophy, definitions, and procedure', *International Journal of Qualitative Methods*, 8, pp. 49–62. doi: 10.2522/ptj.20100192.

John, V. (2015) *Education MEC promises to take Gauteng classrooms into the future*, *Mail&Guardian*. Available at: <http://mg.co.za/article/2015-05-20-education-mec-promises->

- to-take-gauteng-classrooms-into-the-future (Accessed: 27 August 2015).
- Johnson, M. (2012) 'Cybercrime: Threats and Solutions', *Available at SSRN*. Ark Group. Available at: <http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf> (Accessed: 13 January 2015).
- Kabay, M. E. (2002) 'What's Important for Information Security: A Manager's Guide'. Northfield: Norwich University, pp. 1–4.
- Kayle, A. (2011) *SA's security awareness lags*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=42395](http://www.itweb.co.za/index.php?option=com_content&view=article&id=42395).
- Kortjan, N. and Von Solms, R. (2014) 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal*, 52, pp. 29–41. Available at: <http://sacj.cs.uct.ac.za/index.php/sacj/article/view/201/95>.
- Kreutzer, T. (2009) 'Assessing Cell Phone Usage in a South African Township School', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*. Cape Town: e/merge, 5(5), pp. 43–57. Available at: <http://emerge2008.net>.
- Kritzinger, E. (2006) *An Information Security Retrieval And Awareness Model For Industry*. University of South Africa. Available at: <http://uir.unisa.ac.za/bitstream/handle/10500/2475/thesis.pdf?sequence=1>.
- Kritzinger, E. and Padayachee, K. (2007) 'Teaching Safe and Secure usage of ICTs in South African Schools', in *Proceedings of the 2nd International Conference on Society and Information Technologies*. Pretoria, pp. 1–6. Available at: <http://hdl.handle.net/10500/3986>.
- Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security*. Elsevier Ltd, 29(8), pp. 840–847. doi: 10.1016/j.cose.2010.08.001.
- Kruger, H. A., Drevin, L. and Steyn, T. (2006) 'A Framework For Evaluating ICT Security Awareness', in *Information Security for South Africa*, pp. 1–11.
- Kruger, H. a. and Kearney, W. D. (2008) 'Consensus ranking – An ICT security awareness case study', *Computers & Security*. Elsevier Ltd, 27(7–8), pp. 254–259. doi: 10.1016/j.cose.2008.07.001.

- Kyobe, M. (2010) 'Towards a framework to guide compliance with IS security policies and regulations in a university', in *Information Security for South Africa*. Ieee, pp. 1–6. doi: 10.1109/ISSA.2010.5588651.
- Kyobe, M. E., Molai, P. and Salie, T. (2009) 'Investigating electronic records management and compliance with regulatory requirements in a South African university', *SA Journal of Information Management*, 11(1), pp. 1–15. doi: 10.4102/sajim.v11i1.396.
- De Lange, M. and Von Solms, R. (2013) 'An e - Safety Educational Framework in South Africa', in *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Cape Town, p. 497. Available at: [http://www.satnac.org.za/proceedings/2012/papers/3.Internet\\_Services\\_End\\_User\\_Applications/53.pdf](http://www.satnac.org.za/proceedings/2012/papers/3.Internet_Services_End_User_Applications/53.pdf).
- Lau, K. and Albion, P. R. (2010) 'Hong Kong Home Economics Teachers' Adoption of ICT for Learning and Teaching', in Romeo, G. and Gronn, D. (eds) *Digital Diversity Australian Computers in Education Conference 2010*. ACCE. Available at: <http://eprints.usq.edu.au/7354/>.
- Liu, Z., Shu, G. and Lee, D. (2011) *Network Security, Administration and Management*. Edited by D. C. Kar and M. R. Syed. IGI Global. doi: 10.4018/978-1-60960-777-7.
- Maholwana-Sotashe, N. L. (2007) *Challenges faced by secondary school teachers in integrating ICT into the curriculum: A multiple case study in the Grahamstown Circuit*. Rhodes University.
- Mdlongwa, T. (2012) 'Information and Communication Technology ( ICT ) as a Means of Enhancing Education in Schools in South Africa : Challenges , Benefits and Recommendations'. Pretoria: Africa Institute of South Africa, pp. 1–8.
- Mikre, F. (2011) 'The Roles of Information Communication Technologies in Education Review Article with Emphasis to the Computer and Internet', *Ethiopian Journal of Education and Sciences*, 6(2). Available at: <http://www.ajol.info/index.php/ejesc/article/view/73521/62437>.
- Miller, L., Naidoo, M. and Belle, J. Van (2003) 'Critical Success Factors for ICT Interventions in Western Cape Schools'. Cape Town: Department of Information Systems, University of Cape

---

Town, pp. 1–14.

Minister of Justice and Correctional Services (2017) *Cybercrimes and Cybersecurity Bill*.

Republic of South Africa. doi: -.

Moll, I. *et al.* (2007) 'Status Report on ICTs and Higher Education in South Africa'.

Braamfontein: South African Institute for Distance Education (SAIDE). Available at:

[http://www.judybackhouse.com/pdfs/saide\\_status\\_of\\_elearning\\_in\\_sa.pdf](http://www.judybackhouse.com/pdfs/saide_status_of_elearning_in_sa.pdf).

Mullamaa, K. (2010) 'ICT in Language Learning--Benefits and Methodological Implications',

*International Education Studies*, 3(1), pp. 38–44. Available at:

<http://www.ccsenet.org/journal/index.php/ies/article/view/4965/4131>.

MyBroadband (2014) *SA students pour R6.1 billion into tech*. Available at:

<http://businesstech.co.za/news/general/55685/sa-students-pour-r6-1-billion-into-tech/>.

Mzekandaba, S. (2015) *Cybercrime cost SA over R3.42bn in 2013*, *ITWeb Africa*. Available at:

<http://www.itwebafrica.com/security/514-south-africa/234087-cybercrime-cost-sa-over-r342bn-in-2013> (Accessed: 15 March 2015).

Ndlovu, N. S. and Lawrence, D. (2012) 'The quality of ICT use in South African classrooms', in *Towards Carnegie III*. Cape Town: University of Cape Town.

Nevondwe, L. and Odeku, K. O. (2014) 'Protecting Children from Exposure to Pornography in South Africa', *Bangladesh e-Journal of Sociology*, 11(2), pp. 132–142.

Ngcobo, M. (2009) 'A strategic promotion of language use in multilingual South Africa: information and communication', *Southern African Linguistics and Applied Language Studies*, 27(1), pp. 113–120. doi: 10.2989/SALALS.2009.27.1.9.757.

Nyakowa, S. L. (2014) *Factors Influencing ICT Adoption Among Public Secondary School Teachers : A Case of Webuye Sub-County, Bungoma County, Kenya*. University of Nairobi.

Oates, B. J. (2011) *Researching Information Systems and Computing*. London: Sage Publications Ltd.

Olivier, M. S. (2004) *Information Technology Research: A practical guide for Computer Science and Informatics*. 2nd edn. Pretoria: Van Schaik Publishers.

Ope, J. (2014) *An Information Systems Security Framework for Kenyan Public Universities*. University of Nairobi. Available at: <http://erepository.uonbi.ac.ke/handle/11295/76933>

---

(Accessed: 20 January 2015).

Plessis, A. and Webb, P. (2012) 'A Teacher Proposed Heuristic For ICT Professional Teacher Development and Implementation In The South African Context', *Turkish Online Journal of Educational Technology*, 11(4), pp. 46–55.

Poepjes, R. and Lane, M. (2012) 'An Information Security Awareness Capability Model (ISACM)', in *Australian Information Security Management Conference*. Edith Cowan University Research Online. Available at: <http://ro.ecu.edu.au/ism/137>.

PriceWaterhouseCoopers (2010) *Information and Communication Technology for Education in India and South Asia, ICT in School Education (Primary and Secondary)*. Available at: [http://www.infodev.org/infodev-files/resource/InfodevDocuments\\_1016.pdf](http://www.infodev.org/infodev-files/resource/InfodevDocuments_1016.pdf).

Qureshi, I. A., Whitty, M. and Whitty, M. (2014) 'Facebook as e-learning tool for higher education institutes', *Knowledge Management & E-Learning*, 6(4), pp. 440–448.

Radovanovic, D., Radojević, T. and Sarac, M. (2010) 'IT audit in accordance with Cobit standard', in *MIPRO, 2010 Proceedings of the 33rd International Convention*. Opatija, Croatia: IEEE Xplore, pp. 1137–1141. Available at: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5533627](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5533627).

Romm, N. R. A. and Phil, D. L. (2013) 'Employing Questionnaires in terms of a Constructivist Epistemological Stance: Reconsidering Researchers' Involvement in the Unfolding of Social Life', *International Journal of Qualitative Methods*, pp. 652–669.

Rotich, D. C. and Munge, E. M. (2007) 'An overview of electronic information resources sharing initiatives in Kenyan universities', *SA Jnl Libs & Info Sci*, 73(1), pp. 64–74.

Rowe, D. C., Lunt, B. M. and Ekstrom, J. J. (2011) 'The role of cyber-security in information technology education', *Proceedings of the 2011 conference on Information technology education - SIGITE '11*. New York, New York, USA: ACM Press, 2, p. 113. doi: 10.1145/2047594.2047628.

Roy, A. *et al.* (2014) 'Promoting proper education for sustainability: An exploratory study of ICT enhanced Problem Based Learning in a developing country', *International Journal of Education and Development using Information and Communication Technology*, 10(1), pp. 70–90.

- Roy, N. K. (2012) 'ICT-Enabled Rural Education in India', *International Journal of Information and Education Technology*, 2(5), pp. 525–529. doi: 10.7763/IJiet.2012.V2.196.
- Saleh, Z. I., Heba, R. and Mashhour, A. (2011) 'Proposed Framework for Security Risk Assessment', *Journal of Information Security*, 02(02), pp. 85–90. doi: 10.4236/jis.2011.22008.
- Saunders, M., Lewis, P. and Thornhill, A. (2008) *Research Methods for Business Students*, *Research methods for business students*. doi: 10.1007/s13398-014-0173-7.2.
- Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students*. Pearson Education Limited.
- Smit, D. (2015) 'Cyberbullying in South African and American schools: A legal comparative study', *South African Journal of Education*, 35(2), pp. 1–11. doi: 10.15700/saje.v35n2a1076.
- Smith, E. H. and Kruger, H. A. (2010) 'A framework for evaluating IT security investments in a banking environment', in *Information Security for South Africa*. Sandton: IEEE, pp. 1–7. doi: 10.1109/ISSA.2010.5588343.
- Von Solms, S. and Von Solms, R. (2014) 'Towards Cyber Safety Education in Primary Schools in Africa', in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, pp. 185–197.
- Straker, L. *et al.* (2010) 'Evidence-based guidelines for the wise use of computers by children: physical development guidelines.', *Ergonomics*, 53(4), pp. 458–77. doi: 10.1080/00140130903556344.
- Straker, L., Pollock, C. and Maslen, B. (2009) 'Principles for the wise use of computers by children.', *Ergonomics*, 52(11), pp. 1386–401. doi: 10.1080/00140130903067789.
- Surty, M. E. (2011) 'Quality education for rural schools in South Africa – challenges and solutions', *South African Rural Educator*. South Africa: Department of Basic Education, pp. 8–15.
- Swanepoel, A. J. (2015) *Towards A Framework For Understanding Information Systems*. University of Pretoria. doi: 2263/50796.
- The European Network and Information Security Agency (ENISA) (2010) *The new users' guide: How to raise information security awareness*. Available at:

---

[http://www.enisa.europa.eu/publications/archive/copy\\_of\\_new-users-guide](http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide).

UNESCO (2012) 'Why Language Matters for the Millenium Development Goals', in *Language, Education and the Millennium Development Goals*. Bangkok: UNESCO Bangkok.

UNICEF (2012) 'South African mobile generation. Study on South African young people on mobiles', pp. 1–47. doi:

[http://www.unicef.org/southafrica/SAF\\_resources\\_mobilegeneration.pdf](http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf).

Da Veiga, A. (2008) *Cultivating and Assessing Information Security Culture*. University of Pretoria. doi: <http://hdl.handle.net/2263/24117>.

Venktesh, K. (2016) *SA falls in key global ICT index, fintech24*. Available at:

<http://www.fin24.com/Tech/News/sa-falls-in-key-global-ict-index-20161122> (Accessed: 15 May 2017).

Veríssimo, P. and Rodrigues, L. (2001) 'Fundamental Security Concepts', in *Distributed Systems for System Architects*. Springer US, pp. 377–393. doi: 10.1007/978-1-4615-1663-7\_16.

Vermeulen, J. (2014a) *Critical security bug gets SA sites, hosts scrambling, mybroadband*.

Available at: <http://mybroadband.co.za/news/security/100324-critical-security-bug-gets-sa-sites-hosts-scrambling.html>.

Vermeulen, J. (2014b) *New online banking fraud scheme in South Africa, mybroadband*.

Available at: <http://mybroadband.co.za/news/general/100368-new-online-banking-fraud-scheme-in-south-africa.html>.

Walaza, M., Loock, M. and Kritzinger, E. (2014) 'A Framework to Integrate ICT Security Awareness into the South African Schooling System', in *SAICSIT '14 Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology*. Pretoria: ACM, p. 11. doi: 10.1145/2664591.2664596.

Walaza, M., Loock, M. and Kritzinger, E. (2015) 'A Pragmatic Approach towards the Integration of ICT Security Awareness into the South African Education System', in *The Second International Conference on Information Security and Cyber Forensics (InfoSec2015)*. Cape Town, pp. 35–40.

Wayman, I. and Kyobe, M. (2012) 'Incorporating Knowledge of Legal and Ethical Aspects into Computing Curricula of South African Universities', *Journal of Information Technology Education: Innovations in Practice*, 11.

Whitman, M. E. and Mattford, H. J. (2011) *Road Map To Information Security: For IT And InfoSec Managers*. Boston: Course Technology.

## Appendix C: Accepted Research Article – InfoSec2015

**A Pragmatic Approach towards the Integration of ICT Security Awareness into the South African Education System**

Mvelo Walaza, Marianne Loock, Elmarie Kritzinger

School of Computing

University of South Africa

Pretoria, South Africa

53315804@mylife.unisa.ac.za, loockm@unisa.ac.za, kritze@unisa.ac.za

*Abstract* - Information and Communication Technology (ICT) can play a major role in improving the standard of education in South Africa. The increasing use of ICT (mobile phones, PCs, tablets) by South African school learners imposes the need for stringent ICT security awareness initiatives. These initiatives will protect school learners against the dangers associated with growing ICT use. This article presents a practical framework for the integration of ICT security awareness into the South African education system. The framework is called the ICT Security Awareness Framework for Education (ISAFE) and its details are discussed in this article.

***Keywords: ICT security, awareness, education, school learners, models and frameworks, ISAFE***

## **Introduction**

The use of Information and Communication Technology (ICT) among school learners in South Africa is increasing on a daily basis (Kreutzer, 2009). Unfortunately, learners' increased use of technology is accompanied by some degree of danger (such as cyber bullying, cybercrime and child pornography). According to De Lange and Von Solms (De Lange and Von Solms, 2013), it is imperative that children are taught from a young age about the dangers of ICT. This view underscores the importance of the proposed framework, the ISAFE.

According to Walaza, Loock and Kritzinger (Walaza, Loock and Kritzinger, 2014), the ISAFE is constructed using a number of models and frameworks related to ICT in education and ICT security. The models and frameworks for ICT in education that were used are the Teacher Development Framework, the Four-In-Balance Model, and the Model for ICT Rural

Education. The relevant ICT security models and frameworks are the Information Security Retrieval and Awareness (ISRA) model, the Business Model for Information Security, and the Comprehensive Information Security Framework (CISF). The two spheres were compared and analysed in order to arrive at a solution (framework) that includes both sides and is relevant to South Africa.

A gap analysis table was used to analyse the two spheres (ICT in education and ICT security). A number of building blocks (components) to use when constructing the proposed framework were identified and selected from the models and frameworks. Having selected the relevant building blocks from the various models and frameworks with the aim of constructing the proposed framework, a number of components were added, namely Curriculum, Language, Information Repositories and an ICT Security Ombudsman. These new components were added in an attempt to bridge the gap between the two spheres and to make the proposed framework relevant to South Africa. The study reported on in this article presents the proposed framework including the newly added components.

The literature review conducted as part of this study is presented in Section II. The research design is presented in Section III, which covers the problem statement, research questions, objectives, and the potential deliverables of this article. An overview of the ISAFE is presented in Section IV. Lastly, the findings of the research article are presented in Section V and the conclusions in Section VI.

### **Literature Review**

This section presents the literature review that was conducted for this research article. The aim of the literature review is to show the relevance, practicality and effectiveness of the proposed framework.

### **ICT in South Africa**

The use of ICT in South Africa has increased by leaps and bounds over the past couple of years (Dlamini and Modise, 2012). According to UNICEF (UNICEF, 2012), there have been major advances in technology in South Africa; however, there are still challenges with infrastructure and access to the internet. At the time of preparing this article two fixed-line operators (Telkom and Neotel), five mobile operators (Vodacom, Cell C, MTN, Telkom

Mobile and Virgin Mobile), and a large number of Internet Service Providers (ISPs) functioned in the country.

Even though South Africa boasts a large number of internet users and ISPs, there are notable disparities between high- and low-income earners when it comes to technology exposure (Gillwald, Moyo and Stork, 2012). Yet, these disparities have not prevented an enormous increase in the number of users among South African citizens – also those who are still at school. This increasing exposure to ICT raises a concern about the level of ICT security among school learners in South Africa.

### **ICT in South African Education**

South Africa has experienced a huge increase in the use of mobile devices among school learners in the last couple of years (Kreutzer, 2009). School learners use ICT for a variety of purposes such as instant messaging and social media. Distance learning institutes such as the University of South Africa (UNISA), for instance, make use of ICT to communicate with their students who are scattered across the country.

One of the challenges of including ICT in South African education is the lack of adequate ICT skills among school teachers (Kortjan and Von Solms, 2014). Hence it is of utmost importance that school teachers are not excluded when discussing ICT in education.

### **ICT Security Awareness in South African Education**

South Africa, like many other countries, is in need of stringent ICT security awareness initiatives to equip its citizens with much-needed ICT security information. According to Mzekandaba (Mzekandaba, 2015), cybercrime cost South Africa over R3.42 billion in 2013. Efforts to raise ICT security awareness, such as the National Cyber-Security Awareness Week and the South African Cyber-Security Academic Alliance (SACSAA), have fortunately not gone unnoticed (Kortjan and Von Solms, 2014), but they are by far not adequate for solving the problem.

Given the rise in the use of ICT by school learners, it is essential that they are equipped with ICT security knowledge so that they are able to deal with the dangers of ICT. According to Wayman and Kyobe (Wayman and Kyobe, 2012), South Africa has not included the social aspects of ICT in its school curricula. Moreover, Padayachee and Kritzinger (Kritzinger and

Padayachee, 2007), as well as Walaza, Loock and Kritzing (Walaza, Loock and Kritzing, 2014), have called for the inclusion of ICT security awareness training in the South African school curriculum.

### **ICT Safety and Security Models and Frameworks in South Africa**

A number of ICT safety and security models and frameworks have been proposed for South Africa. Walaza, Loock and Kritzing (Walaza, Loock and Kritzing, 2014) used these models and frameworks to formulate the proposed framework, the ISAFE. Some of the frameworks are from South Africa while others were derived from across the globe.

In an effort to increase the level of ICT security awareness, Kortjan and Von Solms (Kortjan and Von Solms, 2014) proposed a conceptual framework for cyber-security awareness and education in South Africa. Kruger et al. (Kruger, Drevin and Steyn, 2006) introduced a framework for evaluating ICT security awareness; whereas Kritzing (Kritzing, 2006) proposed the ISRA model. This shows that scholars have indeed made efforts to contribute to ICT security awareness in South Africa.

### **Research Design**

This section presents the problem statement, research questions and research objectives, as well as the methodology used in this research.

### **Problem Statement**

According to Walaza, Loock and Kritzing (Walaza, Loock and Kritzing, 2014), the main aim of the ISAFE is to integrate ICT security awareness into the South African education system. With the initial framework having been proposed (Walaza, Loock and Kritzing, 2014), the next step is to propose a revised framework that includes all the components (including the newly added ones). Therefore, the problem investigated in this research study can be identified as the lack of integration of ICT security awareness into the South African education system.

The aim of the study was to present the details of the proposed framework and to gauge the feasibility and viability of attempts to integrate ICT security awareness into the South African education system.

The research questions, research objectives and research deliverables are discussed next.

### **Research questions, objectives, and deliverables**

According to Walaza, Loock and Kritzinger (Walaza, Loock and Kritzinger, 2014), the ISAFE aims to integrate ICT security awareness into the South African education system. In order to gauge the practicality and effectiveness of the ISAFE, the research question investigated in the study was formulated as follows:

- Is the proposed framework (the ISAFE) relevant to the South African education system?

The above question enabled the researchers to formulate the research objective as follows:

- To present a framework (the ISAFE) that is relevant to South Africa.

The intended deliverable of this research article was to provide an in-depth literature review regarding the relevance, practicality and effectiveness of the proposed framework. The ISAFE will thus be discussed with the aim of justifying its relevance, practicability and effectiveness in the South African context.

### **Methodology**

The main purpose of the research reported on in this article was to present a framework that can be used to integrate ICT security awareness into the South African education system. As a means to achieve this, an in-depth literature review and analysis was conducted. The literature review focused on the background of the proposed framework and gave an overview of the use of ICT and the level of security awareness in South Africa. The gap analysis that was used to construct the proposed framework is also presented, as well as the ISAFE itself.

The literature review examined the level of ICT use and ICT security awareness in South Africa, as well as ICT security models and frameworks in other countries.

### **Overview of the ISAFE**

This section presents an overview of the ISAFE. The background of the ISAFE is presented in Sub-section A, while the gap analysis and results are shown in Sub-section B. The ISAFE is

depicted and discussed in Sub-section C. Lastly, the relevance of the ISAFE to South Africa is presented in Sub-section D.

### **Background of the ISAFE**

A number of models and frameworks were used during the construction and formulation of the ISAFE. The models and frameworks were divided into two categories, namely the ICT safety and security models and frameworks, and the ICT-in-education models and frameworks. The ICT safety and security models and frameworks are represented in the Business Model for Information Security (ISACA, 2009), the Information Security Retrieval and Awareness (Kritzinger, 2006) model and the Comprehensive Information Security Framework (Da Veiga, 2008). The ICT-in-education models and frameworks are represented in the Four-In-Balance model (Draper, 2010), the Teacher Development Framework (Department of Education, 2007) and the Model for ICT Rural Education (Roy, 2012).

A gap analysis was conducted and it was found that there is indeed a gap between the two categories. This gap is discussed in Sub-section B. The ISAFE was formulated by using a number of relevant components from the various models and frameworks. New components were added to these to make the framework relevant to South Africa.

### **The Gap Analysis and Results**

This section presents the gap analysis that was conducted between the two spheres – ICT safety and security models and frameworks on the one hand and ICT-in-education models and frameworks on the other hand (see Table I).

TABLE 2. THE GAP ANALYSIS

	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>
<b>Leadership and governance</b>		X	X		X	
<b>User awareness</b>	X		X			
<b>Information security documentation</b>	X		X			
<b>Policies and standards</b>			X			
<b>Code of best practice</b>			X			
<b>Human factors</b>		X				X
<b>Collaboration and support</b>		X			X	X
<b>ICT training and learning centres</b>			X			X
<b>Measuring and monitoring</b>	X		X			
<b>Innovation and technology</b>		X		X		
<b>Incident management</b>	X		X			
<b>Compliance</b>			X			
<b>School children</b>		X				X

In Table I, the building blocks that were identified by Walaza, Loock and Kritzing (Walaza, Loock and Kritzing, 2014) are listed in bold in the left-hand column. The different models and frameworks from which the building blocks were taken (marked as A, B, C, D, E, and F) are listed in bold in the top row of Table I:

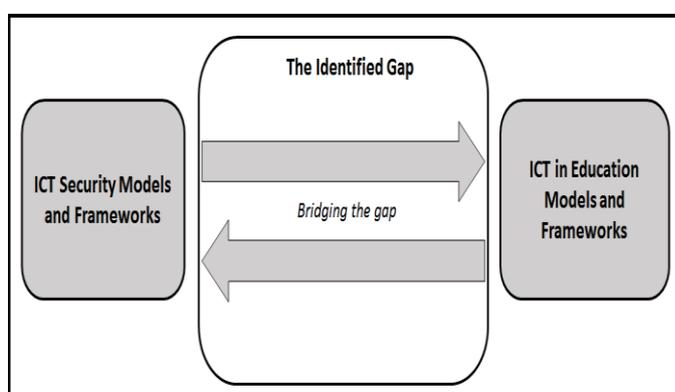
A The Information Security Retrieval and Awareness (ISRA) Model

- B The Business Model for Information Security
- C The Comprehensive Information Security Framework (CISF)
- D The Teacher Development Framework
- E The Four-In-Balance Model
- F The Model for ICT Rural Education

The Leadership & Governance building block was derived from the CISF. It provides the strategy and direction to the implementation of the CISF framework. The User Awareness building block was also derived from the CISF. This building block is responsible for ICT security awareness in this study. The Information Security Documentation building block was derived from the ISRA model. This building block contains all documentation related to information security. The Policies & Standards building block was derived from the CISF. It looks at the best policies and standards that must be adhered to by school learners in South Africa. The Code of Best Practice building block was derived from the CISF. This component investigates the code of best of practice for ICT security in South Africa and encourages school learners to read and adhere to these practices. The Human Factors building block was derived from the Business Model for Information Security. This component investigates some of the factors that might influence ICT security awareness among the South African school learners. The Collaboration & Support building block was derived from the Four In Balance Model. It is used to facilitate the collaboration of ICT security information among institutions in South Africa. The ICT Training & Learning Centres building block was derived from the Model for ICT Rural Education model. This study suggests the formulation and construction of training and learning centres that to assist with ICT security awareness among school learners. The Measuring & Support building block was derived from the ISRA model. It is responsible for the measuring and support of ICT security awareness among school learners in South Africa. The Innovation & Technology building block was derived from both the Teacher Development Framework and the Business Model for Information Security. Its purpose is to promote innovation and technology in order to enhance ICT security awareness among the South African school learners. The Incident Management building block was derived from the CISF framework. It is responsible for the documentation

of all incident management procedures that must be followed by school learners. The Compliance building block was derived from the CISF. Its purpose is to investigate compliance among ICT stakeholders in South Africa, specifically among school learners. The School Learners building block, which is one of the main components of this research study, was derived from the Model for ICT Rural Education model. The researcher proposes that ICT security information and material be made available to the school learners in South Africa on a regular basis using various types of media (such as mobile phones, television, websites, and so on).

The letter “X” marks the building blocks that were encountered in more than one model or framework. As is clear from Table I, there are more building blocks in the ICT security models and frameworks than in the ICT-in-education models and frameworks. This observation allowed the researcher to conclude that there is a gap between the two spheres. Hence, a framework was proposed to integrate ICT security awareness into the South African schooling system. Figure 1 depicts the results of the gap analysis presented in Table I.



*Fig. 1. Gap analysis results*

The clearly visible gap that was encountered between the two spheres prompted the researcher to propose the ISAFE, a framework that would not only bridge this gap, but would also be more practical and relevant in the South African context. The ISAFE is discussed next.

### **The ISAFE**

The framework proposed in this article, namely the ICT Security Awareness Framework for Education (ISAFE), is presented in Figure 2.

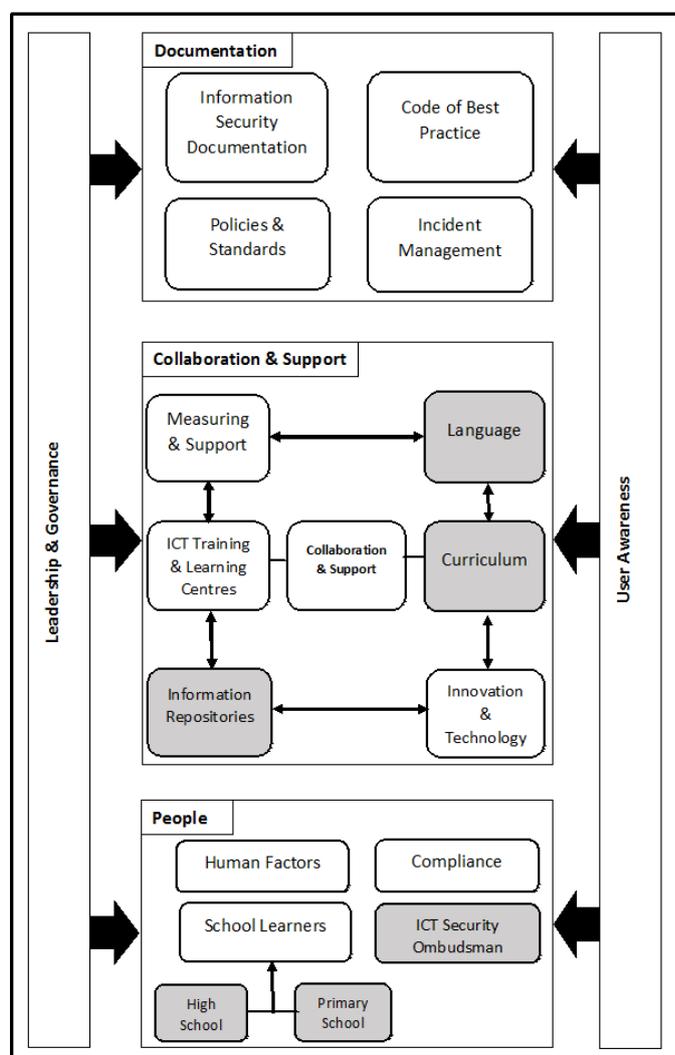


Fig. 2. The ISAFE

The ISAFE is a framework that aims to bridge the gap between the two spheres, namely ICT safety and security models and frameworks and ICT-in-education models and frameworks, and be relevant to South Africa. The framework is comprised of five main components that work together to achieve this goal. These components are Leadership & Governance, User Awareness, Documentation, Collaboration & Support, and People. Each component has various sub-components within itself – used to bridge the previously

mentioned gap between the two spheres and to make the framework relevant to South Africa.

The Leadership & Governance component is responsible for all the governance and the strategic leadership within the framework. The User Awareness component is responsible for all ICT security awareness initiatives proposed by the framework. The Documentation component is responsible for all ICT security awareness related documentation within the framework. The Collaboration & Support is responsible for the integration of the two spheres with the aim of proposing a framework that reflects both spheres. Lastly, the People component is responsible for all the various humanly aspects of the framework, and clearly defines the roles played by each of them.

The components of the ISAFE are all connected via arrows to indicate their interdependence. The joining arrows indicate that no component exists on its own, but that all components work together to achieve the integration of ICT security awareness in South African schools. The newly proposed sub-components are coloured in grey in the framework. This was done to distinguish these components, which were marked as building blocks in Table I, from existing models and frameworks.

### **Relevance of the ISAFE in the South African context**

Language is one of the new components introduced by the ISAFE. It is a very important aspect in South African education, seeing that eleven of the country's languages have official status. According to UNESCO (UNESCO, 2012), research has shown that school learners achieve better grades when they are taught in their mother tongue. This study therefore proposes that ICT security awareness initiatives should be conducted in all the official languages of South Africa.

Another new component added to the framework is Curriculum. This refers specifically to the inclusion of ICT security awareness in the South African school curriculum, which is currently not the case. Scholars such as Von Solms and Von Solms (Von Solms and Von Solms, 2014) have long called for the inclusion of ICT security awareness in the curriculum. This study supports this call and confirms the importance of the proposed ISAFE.

An ICT Security Ombudsman office is another new idea proposed by this study. The rise in the number of ICT-related crimes in South Africa (Belayneh, no date) over the past number of years has reiterated the need for establishing such an office in the country. The current study suggests that an ICT Security Ombudsman office will contribute to and enhance ICT security awareness among school learners in South Africa.

The last component added to the proposed ISAFE is that of Information Repositories. The study proposes that information repositories (such as information-sharing networks and kiosks) should be set up in all public areas such as libraries, hospitals, shopping malls, and many more. Information-sharing networks should be established with the aim of improving and enhancing knowledge among school learners. According to Rotich and Munge (Rotich and Munge, 2007) the creation of information-sharing networks have opened new avenues in Kenya. These information repositories are intended to also contain all the necessary ICT security information that can be used by school learners to enhance their awareness of ICT-related crime.

### **Findings**

The main purpose of the framework proposed in this article is to integrate ICT security awareness into the South African education system. It became evident from the in-depth literature review conducted by the researcher that the existing models and frameworks are not satisfactorily relevant to the South African context and thus a new framework was to be proposed for the country.

The study that was conducted shows that the proposed framework, the ISAFE, with its newly added components, is relevant to South Africa. The new components play a significant role in ensuring that the proposed framework is relevant to South Africa. The study has also managed to bridge the gap that exists between the spheres of ICT-in-education and ICT security models and frameworks.

### **Conclusion**

Even though the literature review that was conducted in this study included other countries, the study was directed towards the South African context. The research reported

on in this article focused on information security awareness in the South African schooling system.

It can therefore be inferred that the proposed framework has achieved its mandate, namely to bridge the gap between the two spheres (ICT in education and ICT security) and to provide a relevant solution for the integration of information security awareness into the South African schooling system.

## References

- Adedayo, W. S. and Ayobami, A. S. (2013) 'Relationship between information security awareness and information security threat', *INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT*, 3, pp. 115–119. Available at: <http://ssrn.com/abstract=2328542>.
- Ahmad, A. (2012) 'Type of Security Threats and It's Prevention.', *International Journal of Computer Technology & Applications*, 3(2), pp. 750–752. Available at: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Type+of+Security+Threats+and+It's+Prevention#0> (Accessed: 13 January 2015).
- Alnatheer, M. and Nelson, K. (2009) 'Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context', in *Proceedings of the 7th Australian Information Security Management Conference*. Security Research Institute Conferences. Available at: <http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1001&context=ism>.
- Aloul, F. A. (2012) 'The Need for Effective Information Security Awareness', *Journal of Advances in Information Technology*, 3(3), pp. 176–183. doi: 10.4304/jait.3.3.176-183.
- Alper, Y. A. (2011) 'Controlling Insider Threats With Information Security Policies', in *ECIS 2011 Proceedings*, pp. 1–12.
- Amedzo, K. E. (2007) *The Integration of Information and Communication technology into Rural Schools of South Africa: A Case Study of Schools in Malamulele*. Stellenbosch University. Available at: <http://scholar.sun.ac.za/handle/10019.1/2135>.
- Andress, J. (2011) *The Basics of Information Security: Understanding the fundamentals of InfoSec in theory and practice*. Edited by Russ Rogers. Waltham: Syngress Press.
- Ashraf, S. (2005) 'Organization Need and Everyone's Responsibility Information Security

- Awareness', *The SANS Institute - Global Information Assurance Certification Paper*, (Security 401).
- Beckers, K., Heisel, M. and Hatebur, D. (2009) 'Supporting Common Criteria Security Analysis with Problem Frames\*', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(300266902), pp. 37–63.
- Belayneh, B. (no date) *South African Centre for Information Security*. Available at: <http://www.sacfis.co.za/index.htm> (Accessed: 14 June 2014).
- Bell ICT Solutions (2007) *The Benefits of ICT*. Available at: <http://www.bell.ca/web/enterprise/newsRoom/en/pdf/Benefits-of-ICT-White-Paper-EN.pdf>.
- Brownson, S. (2014) 'Student Experiential Learning of Cyber Security through Virtualization', *Journal of Research in Innovative Teaching*, 7(1), pp. 112–118.
- Bushati, J. et al. (2012) 'Advantages and Disadvantages of Using ICT in Education', in *International Conference in Europe*, pp. 1–17. Available at: [http://bederweb.majdanov.net/Conferences/ICES 2012/FULL ARTICLE/Bushati\\_Barolli\\_Dibra\\_Haveri\\_Advantages and disadvantages of using ICT in education.pdf](http://bederweb.majdanov.net/Conferences/ICES 2012/FULL ARTICLE/Bushati_Barolli_Dibra_Haveri_Advantages and disadvantages of using ICT in education.pdf).
- Chetty, J. and Coetzee, M. (2010) 'Towards an information security framework for service-oriented architecture', in *Information Security for South Africa*. IEEE, pp. 1–8. doi: 10.1109/ISSA.2010.5588272.
- Chi, M. (2011) 'Security Policy and Social Media Use'. The SANS Institute. Available at: <http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749>.
- Chigona, A. and Chigona, W. (2010) 'An Investigation Of Factors Affecting The Use Of ICT For Teaching In The Western Cape Schools', in *18th European Conference on Information Systems*, p. 12.
- Communications Security Establishment Canada (2013) 'Cyber Security Risks of Using Social Media Guidance for the Government of Canada', pp. 1–2.
- Creswell, J. W. (2009) *Research Design: Qualitative, Quantitative and Mixed Approaches (3rd Edition)*, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. doi:

10.2307/1523157.

Department of Communications (2010) 'The South African Cyber Security Policy', *Government Gazette*, pp. 1–16. doi: <http://dx.doi.org/9771682584003-32963>.

Department of Communications (2014) 'National Integrated ICT Policy Green Paper', *Government Gazette*, 24 January, pp. 3–104. Available at: [www.gpwonline.co.za](http://www.gpwonline.co.za).

Department of Education (2004) 'White Paper on e-Education'. *Government Gazette*, pp. 3–46. Available at:

<http://www.education.gov.za/LinkClick.aspx?fileticket=Keu0%2FBkee%2BM%3D&tabid=191&mid=484>.

Department of Education (2007) 'Guidelines for Teacher Training and Professional Development in ICT'.

Dlamini, Z. and Modise, M. (2012) 'Cyber Security Awareness Initiatives in South Africa: A Synergy Approach', in *7th International Conference on Information Warfare and Security*. Seattle, USA: Academic Conferences International, pp. 62–83. doi: 10.1007/978-3-8349-4134-3\_3.

Dlodlo, N. (2009) 'Access to ICT education for girls and women in rural South Africa: A case study', *Technology in Society*. Pretoria, 31(2), pp. 168–175. doi: doi:10.1016/j.techsoc.2009.03.003.

Draper, K. (2010) *Understanding science teachers' use and integration of ICT in a developing country context*. University of Pretoria. Available at:

<http://upetd.up.ac.za/thesis/available/etd-02032011-132142/unrestricted/thesis.pdf>.

Drevin, L., Kruger, H. A. and Steyn, T. (2007) 'Value-focused assessment of ICT security awareness in an academic environment', *Computers & Security*, 26(1), pp. 36–43. doi: 10.1016/j.cose.2006.10.006.

Edwards, C. K. (2013) *A Framework for the Governance of Information Security, Computers & Security*. Nova Southeastern University. Available at:

<http://www.sciencedirect.com/science/article/pii/S0167404804002639> (Accessed: 26 January 2015).

Fibikova, L. and Mueller, R. (2012) 'Threats, Risks and the Derived Information Security Strategy', in *Securing Electronic Business Processes: Highlights of the Information Security*

- Solutions Europe 2012 Conference (2012)*. Daimler Northeast Asia Ltd, pp. 11–20. doi: 10.1007/978-3-658-00333-3\_2.
- Ford, M. and Botha, A. (2010) 'A Pragmatic Framework for Integrating ICT into Education in South Africa', in Paul Cunningham and Miriam Cunningham (ed.) *IST-Africa 2010 Conference Proceedings*. Port Elizabeth: IIMC International Information Management Corporation, pp. 1–10.
- Fourie, L. and McNamara (2008) *Enhancing the Livelihoods of the Rural Poor Through ICT: A Knowledge Map, South Africa Country Study*. 13. Available at: [http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037\\_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf](http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/11/26/000333037_20081126005327/Rendered/PDF/466280NWP0Box31ica0Country0Study111.pdf).
- Francis, L.-A. (2010) *DOC prioritises cyber security*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=34338:doc-prioritises-cyber-security](http://www.itweb.co.za/index.php?option=com_content&view=article&id=34338:doc-prioritises-cyber-security) (Accessed: 14 June 2014).
- Fu, J. S. (2013) 'ICT in Education : A Critical Literature Review and Its Implications', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 9(1), pp. 112–125.
- Gillwald, A., Moyo, M. and Stork, C. (2012) 'What is happening in ICT in South Africa: A supply-and demand-side analysis of the ICT sector', *Evidence for ICT Policy Action*. Research ICT Africa, (7). Available at: <http://www.researchictafrica.net/docs/Policy Paper 7 - Understanding what is happening in ICT in South Africa.pdf>.
- Gokhe, M. (2000) 'Concept of Information, Communication and Educational Technology', *Thakur Shyamnarayan College of Education and Research (TSCER)*, p. 81. Available at: [http://www.tscermumbai.in/resources\\_paper\\_4/IV.1\\_information\\_and\\_communication\\_technology.pdf](http://www.tscermumbai.in/resources_paper_4/IV.1_information_and_communication_technology.pdf).
- Government of the Hong Kong Special Administrative Region (2008) *An Overview of Information Security Standards, The Government of the Hong Kong Special Administrative Region*. Hong Kong. Available at: <http://www.infosec.gov.hk/english/technical/files/overview.pdf>.
- Grobler, M., Vuuren, J. J. Van and Leenen, L. (2012) 'Implementation of a Cyber Security Policy in South Africa : Reflection on Progress and the Way Forward Current State of Cyber

- Security Research in South Africa', in *ICT Critical Infrastructures and Society*. Amsterdam: Springer Berlin Heidelberg, pp. 215–225. doi: 10.1007/978-3-642-33332-3\_20.
- Grobler, M., Vuuren, J. J. Van and Zaaiman, J. (2011) 'Evaluating Cyber Security Awareness in South Africa', *10th European Conference on Information Warfare and Security ECIW-2011*, pp. 113–121.
- Gundemeda, N. (2014) 'Information Technology (IT) Education in Andhra Pradesh: A Sociological View', *Journal of Social Sciences*, 40(3), pp. 333–342. Available at: [http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemeda-N/JSS-40-3-333-14-1567-Gundemeda-N-Tx\[5\].pdf](http://www.krepublishers.com/02-Journals/JSS/JSS-40-0-000-14-Web/JSS-40-3-14-Abst-PDF/JSS-40-3-333-14-1567-Gundemeda-N/JSS-40-3-333-14-1567-Gundemeda-N-Tx[5].pdf) (Accessed: 2 October 2014).
- Gundu, T. and Flowerday, S. V (2013) 'Ignorance to Awareness: Towards an Information Security Awareness Process', *SAIEE Africa Research Journal*, 104(2), pp. 69–79.
- Hancock, B., Ockleford, E. and Windridge, K. (2009) 'An Introduction to Qualitative Research', *The NIHR RDS EM/YH*. Available at: <http://books.google.cz/books?id=sFv1oWX2DoEC>.
- Higgins, S. (2003) 'Does ICT Improve Learning and Teaching in Schools?', *Journal of Science and Technology*. Bera, 17(6), pp. 586–594. Available at: <http://www.bera.ac.uk/files/reviews/ict-pur-mb-r-f-p-1aug03.pdf>.
- Hong, K. S. and Songan, P. (2011) 'ICT in the changing landscape of higher education in Southeast Asia', *Australasian Journal of Educational Technology*, 27(8), pp. 1276–1290. doi: 10.14742/ajet.893.
- Information Security Resource Center (no date) *Basic Information Security Principles*. Available at: [http://www.oregon.gov/DAS/CIO/ISRC/pages/intro\\_basics.aspx](http://www.oregon.gov/DAS/CIO/ISRC/pages/intro_basics.aspx).
- Internet Service Provider's Association (no date) *419 Scams*. Available at: <http://ispa.org.za/spam/419-scams/>.
- ISACA (2009) *An Introduction to the Business Model for Information Security*. ISACA. Available at: <http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>.
- Isisag, K. U. (2012) 'The Positive Effects of Integrating ICT in Foreign Language Teaching', in *ICT for Language Learning*. Available at: [http://conference.pixel-online.net/ICT4LL2012/common/download/Paper\\_pdf/235-IBT107-FP-Isisag-ICT2012.pdf](http://conference.pixel-online.net/ICT4LL2012/common/download/Paper_pdf/235-IBT107-FP-Isisag-ICT2012.pdf).

- Jabareen, Y. (2009) 'Building a conceptual framework: philosophy, definitions, and procedure', *International Journal of Qualitative Methods*, 8, pp. 49–62. doi: 10.2522/ptj.20100192.
- John, V. (2015) *Education MEC promises to take Gauteng classrooms into the future*, *Mail&Guardian*. Available at: <http://mg.co.za/article/2015-05-20-education-mec-promises-to-take-gauteng-classrooms-into-the-future> (Accessed: 27 August 2015).
- Johnson, M. (2012) 'Cybercrime: Threats and Solutions', Available at SSRN. Ark Group. Available at: <http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf> (Accessed: 13 January 2015).
- Kabay, M. E. (2002) 'What's Important for Information Security: A Manager's Guide'. Northfield: Norwich University, pp. 1–4.
- Kayle, A. (2011) *SA's security awareness lags*. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=42395](http://www.itweb.co.za/index.php?option=com_content&view=article&id=42395).
- Kortjan, N. and Von Solms, R. (2014) 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal*, 52, pp. 29–41. Available at: <http://sacj.cs.uct.ac.za/index.php/sacj/article/view/201/95>.
- Kreutzer, T. (2009) 'Assessing Cell Phone Usage in a South African Township School', *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*. Cape Town: e/merge, 5(5), pp. 43–57. Available at: <http://emerge2008.net>.
- Kritzinger, E. (2006) *An Information Security Retrieval And Awareness Model For Industry*. University of South Africa. Available at: <http://uir.unisa.ac.za/bitstream/handle/10500/2475/thesis.pdf?sequence=1>.
- Kritzinger, E. and Padayachee, K. (2007) 'Teaching Safe and Secure usage of ICTs in South African Schools', in *Proceedings of the 2nd International Conference on Society and Information Technologies*. Pretoria, pp. 1–6. Available at: <http://hdl.handle.net/10500/3986>.
- Kritzinger, E. and Von Solms, S. H. (2010) 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security*. Elsevier Ltd, 29(8), pp. 840–847. doi: 10.1016/j.cose.2010.08.001.
- Kruger, H. A., Drevin, L. and Steyn, T. (2006) 'A Framework For Evaluating ICT Security

---

Awareness', in *Information Security for South Africa*, pp. 1–11.

Kruger, H. a. and Kearney, W. D. (2008) 'Consensus ranking – An ICT security awareness case study', *Computers & Security*. Elsevier Ltd, 27(7–8), pp. 254–259. doi: 10.1016/j.cose.2008.07.001.

Kyobe, M. (2010) 'Towards a framework to guide compliance with IS security policies and regulations in a university', in *Information Security for South Africa*. Ieee, pp. 1–6. doi: 10.1109/ISSA.2010.5588651.

Kyobe, M. E., Molai, P. and Salie, T. (2009) 'Investigating electronic records management and compliance with regulatory requirements in a South African university', *SA Journal of Information Management*, 11(1), pp. 1–15. doi: 10.4102/sajim.v11i1.396.

De Lange, M. and Von Solms, R. (2013) 'An e - Safety Educational Framework in South Africa', in *Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*. Cape Town, p. 497. Available at: [http://www.satnac.org.za/proceedings/2012/papers/3.Internet\\_Services\\_End\\_User\\_Applications/53.pdf](http://www.satnac.org.za/proceedings/2012/papers/3.Internet_Services_End_User_Applications/53.pdf).

Lau, K. and Albion, P. R. (2010) 'Hong Kong Home Economics Teachers' Adoption of ICT for Learning and Teaching', in Romeo, G. and Gronn, D. (eds) *Digital Diversity Australian Computers in Education Conference 2010*. ACCE. Available at: <http://eprints.usq.edu.au/7354/>.

Liu, Z., Shu, G. and Lee, D. (2011) *Network Security, Administration and Management*. Edited by D. C. Kar and M. R. Syed. IGI Global. doi: 10.4018/978-1-60960-777-7.

Maholwana-Sotashe, N. L. (2007) *Challenges faced by secondary school teachers in integrating ICT into the curriculum: A multiple case study in the Grahamstown Circuit*. Rhodes University.

Mdlongwa, T. (2012) 'Information and Communication Technology ( ICT ) as a Means of Enhancing Education in Schools in South Africa : Challenges , Benefits and Recommendations'. Pretoria: Africa Institute of South Africa, pp. 1–8.

Mikre, F. (2011) 'The Roles of Information Communication Technologies in Education Review Article with Emphasis to the Computer and Internet', *Ethiopian Journal of Education and Sciences*, 6(2). Available at:

---

<http://www.ajol.info/index.php/ejesc/article/view/73521/62437>.

Miller, L., Naidoo, M. and Belle, J. Van (2003) 'Critical Success Factors for ICT Interventions in Western Cape Schools'. Cape Town: Department of Information Systems, University of Cape Town, pp. 1–14.

Minister of Justice and Correctional Services (2017) *Cybercrimes and Cybersecurity Bill*. Republic of South Africa. doi: -.

Moll, I. *et al.* (2007) 'Status Report on ICTs and Higher Education in South Africa'.

Braamfontein: South African Institute for Distance Education (SAIDE). Available at:

[http://www.judybackhouse.com/pdfs/saide\\_status\\_of\\_elearning\\_in\\_sa.pdf](http://www.judybackhouse.com/pdfs/saide_status_of_elearning_in_sa.pdf).

Mullamaa, K. (2010) 'ICT in Language Learning--Benefits and Methodological Implications', *International Education Studies*, 3(1), pp. 38–44. Available at:

<http://www.ccsenet.org/journal/index.php/ies/article/view/4965/4131>.

MyBroadband (2014) *SA students pour R6.1 billion into tech*. Available at:

<http://businesstech.co.za/news/general/55685/sa-students-pour-r6-1-billion-into-tech/>.

Mzekandaba, S. (2015) *Cybercrime cost SA over R3.42bn in 2013*, *ITWeb Africa*. Available at:

<http://www.itwebafrica.com/security/514-south-africa/234087-cybercrime-cost-sa-over-r342bn-in-2013> (Accessed: 15 March 2015).

Ndlovu, N. S. and Lawrence, D. (2012) 'The quality of ICT use in South African classrooms', in *Towards Carnegie III*. Cape Town: University of Cape Town.

Nevondwe, L. and Odeku, K. O. (2014) 'Protecting Children from Exposure to Pornography in South Africa', *Bangladesh e-Journal of Sociology*, 11(2), pp. 132–142.

Ngcobo, M. (2009) 'A strategic promotion of language use in multilingual South Africa: information and communication', *Southern African Linguistics and Applied Language Studies*, 27(1), pp. 113–120. doi: 10.2989/SALALS.2009.27.1.9.757.

Nyakowa, S. L. (2014) *Factors Influencing ICT Adoption Among Public Secondary School Teachers : A Case of Webuye Sub-County, Bungoma County, Kenya*. University of Nairobi.

Oates, B. J. (2011) *Researching Information Systems and Computing*. London: Sage Publications Ltd.

Olivier, M. S. (2004) *Information Technology Research: A practical guide for Computer Science and Informatics*. 2nd edn. Pretoria: Van Schaik Publishers.

- Ope, J. (2014) *An Information Systems Security Framework for Kenyan Public Universities*. University of Nairobi. Available at: <http://erepository.uonbi.ac.ke/handle/11295/76933> (Accessed: 20 January 2015).
- Plessis, A. and Webb, P. (2012) 'A Teacher Proposed Heuristic For ICT Professional Teacher Development and Implementation In The South African Context', *Turkish Online Journal of Educational Technology*, 11(4), pp. 46–55.
- Poepjes, R. and Lane, M. (2012) 'An Information Security Awareness Capability Model (ISACM )', in *Australian Information Security Management Conference*. Edith Cowan University Research Online. Available at: <http://ro.ecu.edu.au/ism/137>.
- PriceWaterhouseCoopers (2010) *Information and Communication Technology for Education in India and South Asia, ICT in School Education (Primary and Secondary)*. Available at: [http://www.infodev.org/infodev-files/resource/InfodevDocuments\\_1016.pdf](http://www.infodev.org/infodev-files/resource/InfodevDocuments_1016.pdf).
- Qureshi, I. A., Whitty, M. and Whitty, M. (2014) 'Facebook as e-learning tool for higher education institutes', *Knowledge Management & E-Learning*, 6(4), pp. 440–448.
- Radovanovic, D., Radojević, T. and Sarac, M. (2010) 'IT audit in accordance with Cobit standard', in *MIPRO, 2010 Proceedings of the 33rd International Convention*. Opatija, Croatia: IEEE Xplore, pp. 1137–1141. Available at: [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5533627](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5533627).
- Romm, N. R. A. and Phil, D. L. (2013) 'Employing Questionnaires in terms of a Constructivist Epistemological Stance: Reconsidering Researchers' Involvement in the Unfolding of Social Life', *International Journal of Qualitative Methods*, pp. 652–669.
- Rotich, D. C. and Munge, E. M. (2007) 'An overview of electronic information resources sharing initiatives in Kenyan universities', *SA Jnl Libs & Info Sci*, 73(1), pp. 64–74.
- Rowe, D. C., Lunt, B. M. and Ekstrom, J. J. (2011) 'The role of cyber-security in information technology education', *Proceedings of the 2011 conference on Information technology education - SIGITE '11*. New York, New York, USA: ACM Press, 2, p. 113. doi: 10.1145/2047594.2047628.
- Roy, A. *et al.* (2014) 'Promoting proper education for sustainability: An exploratory study of ICT enhanced Problem Based Learning in a developing country', *International Journal of Education and Development using Information and Communication Technology*, 10(1), pp.

70–90.

Roy, N. K. (2012) 'ICT-Enabled Rural Education in India', *International Journal of Information and Education Technology*, 2(5), pp. 525–529. doi: 10.7763/IJiet.2012.V2.196.

Saleh, Z. I., Heba, R. and Mashhour, A. (2011) 'Proposed Framework for Security Risk Assessment', *Journal of Information Security*, 02(02), pp. 85–90. doi: 10.4236/jis.2011.22008.

Saunders, M., Lewis, P. and Thornhill, A. (2008) *Research Methods for Business Students*, *Research methods for business students*. doi: 10.1007/s13398-014-0173-7.2.

Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students*. Pearson Education Limited.

Smit, D. (2015) 'Cyberbullying in South African and American schools: A legal comparative study', *South African Journal of Education*, 35(2), pp. 1–11. doi: 10.15700/saje.v35n2a1076.

Smith, E. H. and Kruger, H. A. (2010) 'A framework for evaluating IT security investments in a banking environment', in *Information Security for South Africa*. Sandton: IEEE, pp. 1–7. doi: 10.1109/ISSA.2010.5588343.

Von Solms, S. and Von Solms, R. (2014) 'Towards Cyber Safety Education in Primary Schools in Africa', in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, pp. 185–197.

Straker, L. *et al.* (2010) 'Evidence-based guidelines for the wise use of computers by children: physical development guidelines.', *Ergonomics*, 53(4), pp. 458–77. doi: 10.1080/00140130903556344.

Straker, L., Pollock, C. and Maslen, B. (2009) 'Principles for the wise use of computers by children.', *Ergonomics*, 52(11), pp. 1386–401. doi: 10.1080/00140130903067789.

Surty, M. E. (2011) 'Quality education for rural schools in South Africa – challenges and solutions', *South African Rural Educator*. South Africa: Department of Basic Education, pp. 8–15.

Swanepoel, A. J. (2015) *Towards A Framework For Understanding Information Systems*. University of Pretoria. doi: 2263/50796.

The European Network and Information Security Agency (ENISA) (2010) *The new users' guide: How to raise information security awareness*. Available at:

---

[http://www.enisa.europa.eu/publications/archive/copy\\_of\\_new-users-guide](http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide).

UNESCO (2012) 'Why Language Matters for the Millenium Development Goals', in *Language, Education and the Millennium Development Goals*. Bangkok: UNESCO Bangkok.

UNICEF (2012) 'South African mobile generation. Study on South African young people on mobiles', pp. 1–47. doi:

[http://www.unicef.org/southafrica/SAF\\_resources\\_mobilegeneration.pdf](http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf).

Da Veiga, A. (2008) *Cultivating and Assessing Information Security Culture*. University of Pretoria. doi: <http://hdl.handle.net/2263/24117>.

Venktesh, K. (2016) *SA falls in key global ICT index, fintech24*. Available at:

<http://www.fin24.com/Tech/News/sa-falls-in-key-global-ict-index-20161122> (Accessed: 15 May 2017).

Veríssimo, P. and Rodrigues, L. (2001) 'Fundamental Security Concepts', in *Distributed Systems for System Architects*. Springer US, pp. 377–393. doi: 10.1007/978-1-4615-1663-7\_16.

Vermeulen, J. (2014a) *Critical security bug gets SA sites, hosts scrambling, mybroadband*.

Available at: <http://mybroadband.co.za/news/security/100324-critical-security-bug-gets-sa-sites-hosts-scrambling.html>.

Vermeulen, J. (2014b) *New online banking fraud scheme in South Africa, mybroadband*.

Available at: <http://mybroadband.co.za/news/general/100368-new-online-banking-fraud-scheme-in-south-africa.html>.

Walaza, M., Loock, M. and Kritzinger, E. (2014) 'A Framework to Integrate ICT Security Awareness into the South African Schooling System', in *SAICSIT '14 Proceedings of the Southern African Institute for Computer Scientist and Information Technologists Annual Conference 2014 on SAICSIT 2014 Empowered by Technology*. Pretoria: ACM, p. 11. doi: 10.1145/2664591.2664596.

Walaza, M., Loock, M. and Kritzinger, E. (2015) 'A Pragmatic Approach towards the Integration of ICT Security Awareness into the South African Education System', in *The Second International Conference on Information Security and Cyber Forensics (InfoSec2015)*. Cape Town, pp. 35–40.

Wayman, I. and Kyobe, M. (2012) 'Incorporating Knowledge of Legal and Ethical Aspects into

Computing Curricula of South African Universities', *Journal of Information Technology Education: Innovations in Practice*, 11.

Whitman, M. E. and Mattford, H. J. (2011) *Road Map To Information Security: For IT And InfoSec Managers*. Boston: Course Technology.

## Appendix D: Questionnaire

### QUESTIONNAIRE

#### **A Framework to Integrate ICT Safety and Security Awareness into the South African Education**

Dear Participant

Thank you for your willingness to participate in this research study.

- The questionnaire forms part of research currently undertaken by the University of South Africa (UNISA).
- The purpose of the study is to evaluate and analyse the effectiveness and relevance of the ICT Security Awareness Framework for Education (ISAFE) to the South African schooling environment.
- The research has been cleared with the Ethics Committee and CSET at UNISA.
- Your opinion regarding this topic is very valuable to us as this will assist us in analyzing the effectiveness and relevance of the ICT Security Awareness Framework for Education (ISAFE) to the South African schooling environment.
- Please be assured that your privacy and anonymity will be respected and that the information you provide will be treated as highly confidential.
- Please take note that this questionnaire is voluntary and you can withdraw at any time should you so wish with no consequences.
- Information collected from participants will be used exclusively for research purposes (entered as anonymous data).
- To ensure your privacy the questionnaire is anonymous.

- Please fill in the parental consent form and submit it separately. By handing in the consent form separately from your questionnaire your anonymity is guaranteed.
- Please select one option per research question that best describes your perceptions by ticking the appropriate box (except where instructed differently).
- This questionnaire contains 2 sections:  
Section 1: To be completed by the participants.

For more information regarding this project and research topic, please feel free to contact me at any time: [53315804@mylife.unisa.ac.za](mailto:53315804@mylife.unisa.ac.za)

Kind regards

---

Mr. Mvelo Walaza

School of Computing, University of South Africa.

### Introduction

Many countries use Information and Communication Technology (ICT) to improve and enhance the levels and standards of their education systems. A number of scholars in South Africa have conducted studies with the aim of proving that ICT can play a major role in improving the quality of education in the country. This study investigates the problem of the lack of ICT security awareness in South African education (among the South African school learners). The literature review that has been conducted has shown that there is a huge problem when it comes to integrating ICT security awareness into the South African schooling system.

This research project aims to propose a framework to the relevant authorities and interested parties that will assist with the integration of ICT safety and security into the South African schooling system.

I would like to use this opportunity to personally thank you for participating in this research.

**Mr Mvelo Walaza**

**Section 1:**

**To be filled in by all participants**

Section A					
Biographical Information					
	Serial no				
	<div style="border: 1px solid black; display: inline-block; padding: 2px;"> <table border="1" style="border-collapse: collapse;"> <tr> <td style="width: 20px; height: 20px;"></td> </tr> </table> </div> <p style="text-align: right; margin-top: 0;">4</p>				
1.	<p>What is your name and surname? <b>[THIS IS OPTIONAL]</b></p> <hr style="border: 0; border-top: 1px solid black; margin-top: 10px;"/>				
	5				
2.	Your age group:				

	<table border="1"> <tr> <td>1. 20 years and younger</td> <td></td> </tr> <tr> <td>2. 21 – 25 years</td> <td></td> </tr> <tr> <td>3. 26 – 30 years</td> <td></td> </tr> <tr> <td>4. 31 – 35 years</td> <td></td> </tr> <tr> <td>5. 36 – 40 years</td> <td></td> </tr> <tr> <td>6. 41 – 45 years</td> <td></td> </tr> <tr> <td>7. 46 – 50 years</td> <td></td> </tr> <tr> <td>8. 51 – 55 years</td> <td></td> </tr> <tr> <td>9. 56 – 60 years</td> <td></td> </tr> <tr> <td>10. 61 years and older</td> <td></td> </tr> </table>	1. 20 years and younger		2. 21 – 25 years		3. 26 – 30 years		4. 31 – 35 years		5. 36 – 40 years		6. 41 – 45 years		7. 46 – 50 years		8. 51 – 55 years		9. 56 – 60 years		10. 61 years and older		<table border="1"> <tr><td></td></tr> </table> <p>17</p>											
1. 20 years and younger																																	
2. 21 – 25 years																																	
3. 26 – 30 years																																	
4. 31 – 35 years																																	
5. 36 – 40 years																																	
6. 41 – 45 years																																	
7. 46 – 50 years																																	
8. 51 – 55 years																																	
9. 56 – 60 years																																	
10. 61 years and older																																	
<p>3. Your gender:</p>	<table border="1"> <tr> <td>1. male</td> <td></td> </tr> <tr> <td>2. female</td> <td></td> </tr> </table>	1. male		2. female		<table border="1"> <tr> <td></td> </tr> </table> <p>18</p>																											
1. male																																	
2. female																																	
<p>4. Your race:</p>	<table border="1"> <tr> <td>1. black</td> <td></td> </tr> <tr> <td>2. Asian</td> <td></td> </tr> <tr> <td>3. Indian</td> <td></td> </tr> <tr> <td>4. White</td> <td></td> </tr> </table>	1. black		2. Asian		3. Indian		4. White																									
1. black																																	
2. Asian																																	
3. Indian																																	
4. White																																	

	<table border="1"> <tr> <td data-bbox="491 210 799 293">5. Other</td> <td data-bbox="799 210 922 293"></td> </tr> </table>	5. Other		<table border="1"> <tr> <td data-bbox="1259 210 1358 293"></td> <td data-bbox="1358 210 1418 450">19</td> </tr> </table>		19										
5. Other																
	19															
4.	<p>How many years' experience do you have in the Education and/or ICT security industry?</p> <table border="1"> <tr> <td data-bbox="507 748 794 831">1. 5 years and less</td> <td data-bbox="794 748 906 831"></td> </tr> <tr> <td data-bbox="507 831 794 913">2. 6 – 10 years</td> <td data-bbox="794 831 906 913"></td> </tr> <tr> <td data-bbox="507 913 794 996">3. 11 – 15 years</td> <td data-bbox="794 913 906 996"></td> </tr> <tr> <td data-bbox="507 996 794 1079">4. 16 – 20 years</td> <td data-bbox="794 996 906 1079"></td> </tr> <tr> <td data-bbox="507 1079 794 1162">5. 21 – 25 years</td> <td data-bbox="794 1079 906 1162"></td> </tr> <tr> <td data-bbox="507 1162 794 1245">6. 26 years or more</td> <td data-bbox="794 1162 906 1245"></td> </tr> </table>	1. 5 years and less		2. 6 – 10 years		3. 11 – 15 years		4. 16 – 20 years		5. 21 – 25 years		6. 26 years or more		<table border="1"> <tr> <td data-bbox="1259 689 1358 772"></td> <td data-bbox="1358 450 1418 1393">20</td> </tr> </table>		20
1. 5 years and less																
2. 6 – 10 years																
3. 11 – 15 years																
4. 16 – 20 years																
5. 21 – 25 years																
6. 26 years or more																
	20															

<p style="text-align: center;"><b>Section B</b></p> <p style="text-align: center;"><b>The Proposed Framework</b></p>				
<p>5 Do you think there is a problem with the integration of ICT into the South African education system? Please elaborate.</p> <table border="1"> <tr> <td data-bbox="491 1937 608 2020">1. yes</td> <td data-bbox="608 1937 724 2020"></td> </tr> </table>	1. yes		<table border="1"> <tr> <td data-bbox="1449 1957 1485 2033"></td> </tr> </table>	
1. yes				



7	<p>In your opinion, is the proposed framework understandable and easy to read?</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <tr> <td style="padding: 5px;">1. yes</td> <td style="width: 40px;"></td> </tr> <tr> <td style="padding: 5px;">2. no</td> <td></td> </tr> </table> <p>If you selected 'No', then what can be improved?</p> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>	1. yes		2. no		<div style="border: 1px solid black; width: 20px; height: 20px; margin: 0 auto;"></div> <p>24</p>
1. yes						
2. no						
9	<p>Does the proposed framework address the problem of lack of ICT safety and security awareness in South African schooling system?</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <tr> <td style="padding: 5px;">1. Yes</td> <td style="width: 40px;"></td> </tr> <tr> <td style="padding: 5px;">2. No</td> <td></td> </tr> </table>	1. Yes		2. No		<div style="border: 1px solid black; width: 20px; height: 20px; margin: 0 auto;"></div> <p>35</p>
1. Yes						
2. No						
1	<p>Does the framework address all aspects regarding the lack of ICT security awareness in the South African schooling environment?</p> <table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <tr> <td style="padding: 5px;">1. Yes</td> <td style="width: 40px;"></td> </tr> <tr> <td style="padding: 5px;">2. No</td> <td></td> </tr> </table>	1. Yes		2. No		<div style="border: 1px solid black; width: 20px; height: 20px; margin: 0 auto;"></div> <p>36</p>
1. Yes						
2. No						
1	<p>In your opinion, will the proposed framework make a meaningful contribution towards</p>					



	<table border="1" data-bbox="491 208 722 371"> <tr> <td data-bbox="491 208 608 286">1. Yes</td> <td data-bbox="608 208 722 286"></td> </tr> <tr> <td data-bbox="491 286 608 371">2. No</td> <td data-bbox="608 286 722 371"></td> </tr> </table>	1. Yes		2. No		
1. Yes						
2. No						
1	<p data-bbox="220 539 1318 629">Do you think the proposed framework will make a meaningful contribution towards the South African education system?</p> <table border="1" data-bbox="491 831 722 994"> <tr> <td data-bbox="491 831 608 909">1. Yes</td> <td data-bbox="608 831 722 909"></td> </tr> <tr> <td data-bbox="491 909 608 994">2. No</td> <td data-bbox="608 909 722 994"></td> </tr> </table>	1. Yes		2. No		<div data-bbox="1449 613 1485 696" style="border: 1px solid black; width: 20px; height: 20px; margin: 0 auto;"></div> <p data-bbox="1449 701 1485 730" style="text-align: center;">39</p>
1. Yes						
2. No						
1	<p data-bbox="220 1160 1337 1249">Are the components (building blocks) of this framework relevant to the South African context?</p> <table border="1" data-bbox="491 1451 722 1615"> <tr> <td data-bbox="491 1451 608 1529">1. Yes</td> <td data-bbox="608 1451 722 1529"></td> </tr> <tr> <td data-bbox="491 1529 608 1615">2. No</td> <td data-bbox="608 1529 722 1615"></td> </tr> </table>	1. Yes		2. No		<div data-bbox="1449 1234 1485 1317" style="border: 1px solid black; width: 20px; height: 20px; margin: 0 auto;"></div> <p data-bbox="1449 1321 1485 1350" style="text-align: center;">40</p>
1. Yes						
2. No						
1	<p data-bbox="220 1780 1281 1870">Does the proposed framework make a meaningful contribution to the field of ICT security in Education?</p>	<div data-bbox="1449 1854 1485 1937" style="border: 1px solid black; width: 20px; height: 20px; margin: 0 auto;"></div> <p data-bbox="1449 1942 1485 1971" style="text-align: center;">41</p>				



<hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>					
<p>1 What is your overall rating of the proposed framework (out of a 100)?</p> <table border="1" data-bbox="491 927 722 1093"> <tr> <td>1. Yes</td> <td></td> </tr> <tr> <td>2. No</td> <td></td> </tr> </table>	1. Yes		2. No		<div style="text-align: center;"> <input style="width: 20px; height: 20px;" type="text"/>              44         </div>
1. Yes					
2. No					
<p>1 Are you satisfied with the contribution that the researcher has done to formulate this framework?</p> <table border="1" data-bbox="491 1469 722 1635"> <tr> <td>1. Yes</td> <td></td> </tr> <tr> <td>2. No</td> <td></td> </tr> </table>	1. Yes		2. No		<div style="text-align: center;"> <input style="width: 20px; height: 20px;" type="text"/>              45         </div>
1. Yes					
2. No					

Thank you for your participation.