

**TOWARDS A CYBER SAFETY INFORMATION FRAMEWORK FOR SOUTH AFRICAN
PARENTS**

By

Elvira Libabat Paraiso

15260772

Submitted in fulfilment of the requirements for the degree

M IT in Information Systems

In the

FACULTY OF ENGINEERING BUILT AND INFORMATION TECHNOLOGY

At the

UNIVERSITY OF PRETORIA

Study leader:

Prof M. C. Matthee

Date of submission

31 January 2019

Declaration regarding Plagiarism

The Department of Informatics emphasises integrity and ethical behaviour with regard to the preparation of all written assignments.

Although the lecturer will provide you with information regarding reference techniques, as well as ways to avoid plagiarism, you also have a responsibility to fulfil in this regard. Should you at any time feel unsure about the requirements, you must consult the lecturer concerned before submitting an assignment.

You are guilty of plagiarism when you extract information from a book, article, web page or any other information source without acknowledging the source and pretend that it is your own work. This does not only apply to cases where you quote verbatim but also when you present someone else's work in a somewhat amended (paraphrased) format or when you use someone else's arguments or ideas without the necessary acknowledgement. You are also guilty of plagiarism if you copy and paste information directly from an electronic source (e.g., a website, e-mail message, electronic journal article, or CD ROM), even if you acknowledge the source.

You are not allowed to submit another student's previous work as your own. You are furthermore not allowed to let anyone copy or use your work with the intention of presenting it as his/her own.

Students who are guilty of plagiarism will forfeit all credits for the work concerned. In addition, the matter will be referred to the Committee for Discipline (Students) for a ruling. Plagiarism is considered a serious violation of the University's regulations and may lead to your suspension from the University. The University's policy regarding plagiarism is available on the Internet at <http://upetd.up.ac.za/authors/create/plagiarism/students.htm>.

I (full names & surname):	Elvira Libabat Paraiso
Student number:	15260772

Declare the following:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. I declare that this assignment is my own, original work. Where someone else's work was used (whether from a printed source, the Internet or any other source) due acknowledgement was given and reference was made according to departmental requirements.
3. I did not copy and paste any information directly from an electronic source (e.g., a web page, electronic journal article or CD ROM) into this document.
4. I did not make use of another student's previous work and submitted it as my own.
5. I did not allow and will not allow anyone to copy my work with the intention of presenting it as his/her own work.

ELP

Signature

31/01/2019

Date

TABLE OF CONTENTS

1	INTRODUCTION	2
1.1	BACKGROUND	3
1.2	PROBLEM STATEMENT	7
1.3	RESEARCH QUESTIONS.....	8
1.4	PURPOSE OF THE STUDY	9
1.5	ASSUMPTIONS.....	10
1.6	SHORT DEFINITION OF MAIN TERMS AND CONCEPTS	10
1.7	RESEARCH APPROACH.....	11
1.8	DISSERTATION LAYOUT	11
1.9	SUMMARY	13
2	LITERATURE REVIEW	14
2.1	INTRODUCTION	14
2.2	DIGITAL CITIZENSHIP	14
2.3	CYBER ETHICS	16
2.4	CYBER SECURITY	18
2.4.1	Cyber Security Overview.....	18
2.4.2	Towards Raising Cyber Security Awareness	20
2.5	CYBER SAFETY	21
2.5.1	Cyber Safety Threats	22
2.5.2	Cyber Safety Skills and Digital Literacy.....	30
2.5.3	Parents, Teachers and Cyber Safety	31
2.5.4	Towards Raising Parents Cyber Safety Awareness.....	32
2.6	CYBER SAFETY FRAMEWORKS	43

2.6.1	A Framework for Cyber Security in Africa	43
2.6.2	National Safe Schools Framework	45
2.6.3	Framework for an African Policy towards Creating Cyber Security Awareness 47	
2.6.4	High-Level e-Safety Framework.....	49
2.7	DISSEMINATING FORMATS AND CONTENTS FOR CYBER SAFETY AWARENESS CAMPAIGNS	52
2.8	CONCLUSION.....	55
3	METHODOLOGY	57
3.1	INTRODUCTION	57
3.2	RESEARCH DESIGN	57
3.2.1	Research Paradigm	57
3.2.2	Design Science Research.....	59
3.2.3	Design Science Research Guidelines	60
3.2.4	Design Science Research Methodology	62
3.3	DESIGN SCIENCE RESEARCH METHODOLOGY APPLICATION	67
3.3.1	Main Cycle	69
3.3.2	Sub-Cycle 1 – A Cyber Safety Information Needs Assessment Instrument (CSINAI) for Parents.....	73
3.3.3	Sub-Cycle 2 – A Categorisation of Existing Cyber Safety Information for Parents81	
3.3.4	Summary of Research Approach	83
3.4	ETHICAL CONSIDERATIONS	85
3.5	CONCLUSION.....	86
4	AWARENESS AND SUGGESTION – MAIN CYCLE.....	87
4.1	AWARENESS – NEED FOR A CYBER SAFETY INFORMATION FRAMEWORK FOR PARENTS.....	87
4.1.1	Awareness Overview	87
4.1.2	Awareness Campaign Overview	88

4.2	SUGGESTION.....	89
4.2.1	Preliminary Cyber Safety Information Framework.....	89
4.3	CONCLUSION.....	92
5	DEVELOPMENT – SUB-CYCLE 1: CYBER SAFETY INFORMATION NEEDS ASSESSMENT INSTRUMENT.....	94
5.1	AWARENESS.....	94
5.2	SUGGESTION.....	94
5.3	DEVELOPMENT.....	95
5.4	EVALUATION.....	96
5.4.1	Interview Results.....	96
5.4.2	Questionnaire Results.....	99
5.4.3	Revising the Cyber Safety Information Needs Assessment Instrument (CSINAI).....	100
5.4.4	How to Apply the Cyber Safety Information Needs Assessment Instrument (CSINAI).....	100
5.5	SUMMARY.....	104
6	DEVELOPMENT – SUB-CYCLE 2: CATEGORISATION OF EXISTING CYBER SAFETY INFORMATION FOR PARENTS AND UPDATED VERSION OF THE FRAMEWORK.....	105
6.1	DEVELOPMENT – SUB-CYCLE 2: CATEGORISATION OF EXISTING CYBER SAFETY INFORMATION FOR PARENTS.....	105
6.1.1	Awareness.....	105
6.1.2	Suggestion.....	105
6.1.3	Development.....	106
6.2	DEVELOPMENT – MAIN CYCLE: UPDATED VERSION OF THE CYBER SAFETY INFORMATION FRAMEWORK.....	111
6.2.1	Introduction.....	111
6.2.2	Updated Cyber Safety Information Framework.....	111
6.3	SUMMARY.....	112

7	EVALUATION – MAIN CYCLE	113
7.1	THE APPLICATION OF THE CYBER SAFETY INFORMATION FRAMEWORK 113	
7.1.1	Cyber Safety Awareness Form	114
7.1.2	Database.....	115
7.2	EVALUATION FEEDBACK.....	117
7.2.1	Evaluation Criteria.....	117
7.2.2	Feedback	117
7.2.3	Refinements.....	120
7.3	CONCLUSION.....	122
8	CONCLUSION – MAIN CYCLE	123
8.1	RESPONSES TO RESEARCH QUESTIONS	123
8.1.1	Sub Research Questions	123
8.1.2	Main Research Question.....	125
8.2	LIMITATIONS	125
8.3	COMMUNICATION OF THE ARTEFACT AND FUTURE RESEARCH.....	126
8.3.1	Communication of the Artefact.....	126
8.3.2	Future Research	127
9	REFERENCES	128
10	APPENDICES.....	143
10.1	APPENDIX A: QUESTIONNAIRE AND ETHICS APPROVAL	143
10.2	APPENDIX B: RESULTS OBTAINED FROM QUESTIONNAIRE	152
10.3	APPENDIX C: FINAL VERSION OF THE CSINAI SHARED WITH REPRESENTATIVE	154
10.4	APPENDIX D: CYBER SAFETY AWARENESS MANUAL.....	160
10.5	APPENDIX E: REVISED VERSIONS OF CSINAI AND CYBER SAFETY AWARENESS FORM SHARED TO PUBLIC	174
10.5.1	Layout + Code of the Cyber Safety Awareness Form.....	174

10.5.2	Final CSINAI	177
--------	--------------------	-----

LIST OF TABLES

Table 1	Dissertation Layout	12
Table 2	Summary of Data Collection and Analysis Approaches in Sub-Cycle 1	76
Table 3	Summary of Data Collection and Analysis Approaches in Sub-Cycle 2	83
Table 4	Summary of the Research Approach	83
Table 5	Component of Cyber Safety Awareness Campaign	88
Table 6	Framework Components (Adapted from de Lange and von Solms (2012)	90
Table 7	Extension Criteria for the Targeted Audience Only (Parents)	91
Table 8	Interview Results	97
Table 9	Results of the Cyber Safety Information Needs Assessment Instrument	99
Table 10	Results Equivalent for Section 1	101
Table 11	Results Equivalent for Section 2	101
Table 12	Results Equivalent for Section 3	102
Table 13	Application of Results of the Questionnaire Inspired by Table 9's Results	103
Table 14	Categorisation Framework	107
Table 15	Categorisation According to School X Parents' Needs	110

LIST OF FIGURES

Figure 1 High-Level Information Menu.....	33
Figure 2 Online Threats Menu	34
Figure 3 Cyberbullying Information on Esafety.gov.au	34
Figure 4 Procedures to Report Cyberbullying from Esafety.gov.au	35
Figure 5 Parents Guide to Online Safety (SA Health, 2013).....	36
Figure 6 Example of Acronyms Used by Children from (CyberAngels; Time Warner Cable, 2007).....	37
Figure 7 Parents Links to Useful Resources to Help with their Conversation with Children and Increase their Knowledge on the Matter (UK Safer Internet Centre, 2016)	38
Figure 8 African Social Programmes and Initiatives – Home	39
Figure 9 OnTRAC Support System.....	40
Figure 10 Quiz on Internet Safety; internetsafety.org.za/quiz/	41
Figure 11 Proposed Comprehensive Framework for Cyber Safety by Kritzinger and von Solms (2012).....	44
Figure 12 Cyber Security Awareness Framework proposed by Dlamini, Taute and Radebe (2011)	47
Figure 13 High-Level e-Safety Framework, de Lange & von Solms (2012)	49
Figure 14 Menu According to Intended Audience (US National Center for Missing & Exploited Children, 2016).....	53
Figure 15 Menu According to the Age of Children (UK Safer Internet Centre, 2016).....	53
Figure 17 Overview of the Design Science Research Methodology steps (Vaishnavi and Kuechler, 2007).....	63
Figure 16 ISTQB Exam Certification - Prototyping Model (ISTQB Exam Certification, n.d.)	65
Figure 18 Design Science Research Methodology Application (adopted from (Vaishnavi and Kuechler, 2007).....	68
Figure 19 Overview of the Outcomes of Each Step of the Dissertation’s Design Science Research Methodology (Vaishnavi and Kuechler, 2007)	69

Figure 20 Adaptation of Design Science Research Cycles According to Our Research (Hevner, 2007)	73
Figure 21 The Different Design Science Research Methodology Phases of Sub-Cycle 1	74
Figure 22 The Different Design Science Research Methodology Phases of Sub-Cycle 2	81
Figure 23 Preliminary Cyber Safety Information Framework	92
Figure 24 Updated Cyber Safety Information Framework.....	112
Figure 25 Preliminary Cyber Safety Awareness Form	115
Figure 26 Database's ERD	117
Figure 27 Final Cyber Safety Awareness Form	121
Figure 28 Final Version of the Cyber Safety Information Framework	125

TOWARDS A CYBER SAFETY INFORMATION FRAMEWORK FOR SOUTH AFRICAN PARENTS

ABSTRACT

This dissertation addresses the need for a structured approach to the education of parents regarding cyber safety threats. The researcher has been approached by a service provider, EduX, which works with schools to facilitate digital learning. Edu X has expressed the need to provide cyber safety information for parents from the schools where their solution is implemented. This research suggests a Cyber Safety Information Framework for South African parents, tailored to their specific needs.

The Design Science Research Methodology was followed to develop the framework through one main cycle and two sub-cycles. The framework includes different dimensions of the parents' needs. A Cyber Safety Information Needs Assessment Instrument was developed and tested to tailor these dimensions to a specific school. In addition, a categorisation (or catalogue) of existing cyber safety online material to be used by schools, was developed. The evaluation of this framework was done by designing a prototype of an application to be used by schools to determine its implementation based on the outcome of the needs assessment instrument, the relevant cyber safety content, the way to present the material, as well as the best time to present it. This prototype was demonstrated to a potential user from EduX, and the framework was refined and updated based on the feedback received.

Keywords: Parents' Awareness, Cyber Safety, Framework, Cyber Safety Education, Design Science Research

1 INTRODUCTION

The advancement of mobile technology, with ever-increasing improvements and affordability, has evolved the way society communicates, socialises and learns (Pollara, 2011). Almost anyone can have a cell phone that connects to the internet nowadays and take full advantage of the vast opportunities offered. During the last decade, the utilisation of the internet and technological devices used for communication (such as mobile phones and tablets) has revolutionised education and the way the world learns (Kambourakis, 2013). Some schools even provide the devices for their learners to encourage this modern form of learning (Voigt & Matthee, 2012). This is highly beneficial for the world human beings are currently living in, as it sets out to produce and educate technology-savvy individuals.

Martin and Ertzberger (2013) suggested that using mobile devices for learning purposes could either aid or limit the learning experience. Using mobile devices aids education because learning can take place whenever it is needed (Ally, 2004), and is no longer restricted to a classroom (Johnson, Adams & Cummins, 2012). Some students consider the use of mobile devices as beneficial to their education, as it encourages learning during leisure time between lectures and at home (Maifarth, et al., 2013). However, the learning experience can be constrained due to the risks that learners are exposed to while using mobile devices and the internet, such as a breach of their security and safety (Sharples, 2006). Learners can be unprotected and come across inappropriate content like pornography or potentially dangerous people like stalkers and paedophiles, or be exposed to cyberbullying, fraud and viruses.

Students need to be taught how to be (and remain) safe online to take full advantage of this modern learning experience, as well as how not to cause any harm to themselves or others online. Learners need to be made aware of the cyber safety dangers they may encounter, and how to tackle them. Parents play a crucial role in their children's cyber safety education, but for it to be effective, they need to be educated and well-informed themselves. One realises that some parents are not aware of the full extent of what can happen online (African Social Programmes and Initiatives, 2015), as well as what should be done to educate their

INTRODUCTION

children (de Lange & von Solms, 2012). Parents, therefore, need information that will help them become aware of cyber safety, so that parents can be effectual educators and leaders.

The Digital Citizenship and Safety Project was an initiative run by UNICEF in 2011. Their primary objective was to engage with young adults in various countries to master traditional and new technologies, so parents can become productive members of modern society. Modelled along the lines of this project, UNICEF conducted a study in South Africa where informative materials were developed and distributed to increase the awareness of young people around safe and responsible use of the internet and communication technology devices. UNICEF concluded that South African organisations and the government are actively promoting online safety, but given the fast-growing number of ICT users, there is a need for well-structured laws and educational materials, especially for new users (Beger & Sinha, 2012).

This research will contribute towards the research on cyber safety education in South Africa (with the focus on parental awareness) using the published literature review, along with an empirical study. The study will identify the most common cyber safety issues learners and their parents encounter. The study will also determine the level of awareness of a selected group of parents and identify gaps and future educational needs. With the use of a design science research methodology, this research will help to provide a cyber safety information framework that can be used to develop an awareness guide or campaign. This framework can be utilised by service providers of mobile and e-learning solutions, as they can offer it (in addition to their services) to schools to educate and build cyber-alert citizens. In conjunction with teachers, parents will also be part of that teaching process. This framework is meant for parents to help make them aware of what can happen online, and how parents can assist their children. It will extend the cyber safety education in schools to the children's homes and private lives, encouraging a safe and secure cyber environment for everyone.

1.1 BACKGROUND

One is living in an era of technological revolution. Mobile devices have gone from being luxury items to being a necessity (Pollara, 2011). No longer used only for communication,

INTRODUCTION

the advancement of technology has seen mobile devices find their way into schools and educational programs the world over (Shonola & Joy, 2014), transforming the way the world learns.

The use of mobile devices in education unlocks unlimited opportunities for learning at any time, in any place (Johnson, et al., 2012). Technology can enhance the learning experience (Padayachee, 2011) by providing learners with access to interactive content and multiple online digital learning tools. Getting in contact with teachers and fellow pupils is made easier through the use of mobile devices in schools, making educational assistance immediate and more effective.

According to Looi, Sun and Xie (2014), some cases have shown that the use of mobile devices improves the grades of learners, as it enhances their interest in learning and sharing knowledge. However, this advancement is not without its issues and concerns. Improper use of this vast and universal learning experience exposes students to potentially risky situations, especially regarding their privacy and safety (Sharples, 2006). Learners, particularly children, are exceedingly vulnerable while using mobile devices, due to their curiosity and enthusiasm when introduced to new technologies (von Solms & von Solms, 2014). Risky situations may involve being exposed to inappropriate content or violence, development of a negative self-image and cyberbullying. Sometimes, students are unaware that private information such as their location, browsing history and IP addresses may be shared with a third party without their consent (Kambourakis, 2013). There may be no control over who the third party is, increasing the threat of predators.

Digital learning devices allow the monitoring of learners by their teachers and parents, ensuring learners are doing what they are supposed to be doing on their devices at any given time. Although this monitoring is said to be for the students' safety, it might become blurry and cross the fine line between invading their privacy and protecting them (Traxler, 2010). People with ill-intent may also intercept this information, which is potentially dangerous. Considering children's vulnerability, it is crucial to ensure their safety while online (Padayachee, 2011).

INTRODUCTION

Compared to other major African countries such as Zambia, Cameroon, Namibia, Tanzania and Uganda, South Africa has a more significant number of users of mobile devices, the internet, social media and networking on the continent (Beger & Sinha, 2012). Burton & Mutongwizo (2009) have shown that, from the sample surveyed in their study in South Africa, 92.9% of people between the ages of 12 and 24 years old possess or have access to a mobile device. The increasing affordability of mobile devices with internet access, coupled with the decreasing prices of internet data bundles, has expanded the number of young people who have access to the web in South Africa (Popovac & Leoschut, 2012). Recent research conducted by Kritzinger (2014) on 503 South African children between the ages of 16 and 19, reported that:

- 35 % of children (respondents) hide what they are doing online from their parents or guardian
- 63% of children have come across inappropriate internet material like pornography
- 93% of children believed that possible threats related to internet use exist
- 15% of children used their mobile phones during school hours, even if it is against the school's rules
- 61% of children indicated that neither parents nor teachers were monitoring their activities on the internet. Additionally, most of them specified that no parental guidance software was installed to regulate their internet access

With the introduction of mobile devices for learning purposes, students are being more and more exposed to the advantages and disadvantages of digital learning platforms, especially concerning their privacy and safety. Learners are now able to acquire knowledge from an infinite number of sources at any given time (Ally, 2004). While learning, pupils may be exposed to non-relevant content or potentially dangerous individuals such as stalkers and paedophiles; or encounter issues like violence, cyberbullying and excessive monitoring. As an example, cyberbullying (also known as internet bullying) is a type of bullying that occurs using the web or mobile devices (Vanderbosh & Van Cleemput, 2008). Learners, especially females, view cyberbullying as a problem that is not being prioritised and thoroughly discussed by teachers or parents (Agatston, et al., 2007). Children feel that their parents and teachers are not well-informed on the matter or how they should react to or avoid it.

INTRODUCTION

Cyber safety may be defined as when the internet and technological devices are utilised wisely and responsibly (Australian Communications and Media Authority, 2010). Six individuals have been identified as the most critical role-players in cyber safety awareness and education: governments' actions, law enforcement, parents, schools, teachers and peers (von Solms & von Solms, 2015). However, some believe that schools might be the most effective place for cyber safety awareness to be taught but should not be the only one. Parents of learners play a major role in the cyber safety education of their children (von Solms & von Solms, 2014). Schools are, most of the time, believed not to be fully equipped in assisting parents facing the consequences of the use of mobile devices in education, as well as in encouraging and promoting cyber safety (Australian Communications and Media Authority, 2010). Parents should be able to continue the education provided by the school at home or should be proactive in introducing their children to cyber safety to ensure everybody's safety online. de Lange & von Solms (2012) found that most parents are not entirely aware of the cyber safety issues that may be associated with the utilisation of mobile devices and the internet, and how their child is behaving online. This may be attributed to the fact that most parents were born before the development of the technology and may be trying to adapt to it without definitive guidance themselves (van Niekerk, et al., 2013). As a result, parents would not be informed enough to guide the cyber safety education of their children at home.

These findings substantiate the fact that children do not possess the required online safety skills, and even if children do, there is no serious monitoring to ensure kids apply what has been taught to them. Hence, learners need to be taught the skills required to benefit fully from the use of mobile devices, while remaining secure and responsible under supervision at school and, more importantly, at home. Some parents, however, appear not to be knowledgeable enough to continue the cyber education given at school (de Lange & von Solms, 2012). Many parents are often less knowledgeable about technology than their children (Computer Science and Telecommunications Board - National Research Council, 2002), and often feel overwhelmed by their children's new learning and social environments (Hollingworth, et al., 2009). Hence, it is important that parents receive guidelines around cyber safety to facilitate their understanding of the platform and improve the quality of the guidance offered to their children.

1.2 PROBLEM STATEMENT

In South Africa, learners between 12 and 24 years old are increasingly exposed to the internet, primarily via mobile devices that these learners own or have access to (Burton & Mutongwizo, 2009). Although organisations are actively encouraging cyber safety, there is a lack of well-structured approaches for schools, teachers and parents to help them in reacting to, or avoiding, cyber threats (Sonhera, et al., 2012). South Africa, in particular, lacks strategies relevant to the South African context (Kortjan & von Solms, 2014). Furthermore, the researchers noticed that parents and teachers do not have access to customised programmes to assist children (von Solms & von Solms, 2014), which results in their general lack of knowledge and skills about Information and Communication Technology (ICT) and its challenges. Because of this, it would be invaluable to investigate the type of cyber safety issues that may be encountered when implementing the use of mobile devices in educational environments, as well as what South African parents should know to encourage better and enhance their children's cyber safety awareness. South African teachers and parents have limited access to information and policies to assist their children (von Solms & von Solms, 2014) regarding ICT use. At the same time, the majority of African countries, including South Africa, do not have initiatives for raising cyber safety awareness for children, parents and teachers (von Solms & von Solms, 2014). The high level of digital illiteracy in South Africa, in conjunction with insufficient access to ICT infrastructures, the language barrier and the geographic location of individuals, has a substantial impact on cyber safety awareness (Kritzinger, 2015).

In European countries, parents with lower levels of digital literacy tend to be more restrictive towards the use of the internet by their children, and may therefore, be restricting the learning and online exploration of their children. Those parents with higher levels of digital literacy tend to embrace technology with their children and guide them more efficiently (Duerager & Livingstone, 2012). Duerager & Livingstone (2012), recommend that instead of restricting the internet usage of their children, parents need to embrace technology and actively partake in their children's online experience. Parents need to discuss the possible dangers with their children, engage in their children's internet use and set age-appropriate rules. Parents with lower digital literacy, from both developing and developed countries, may struggle to advise their children on adopting appropriate online behaviour, instead of

INTRODUCTION

allowing them to discover the internet on their own. The parents that are more informed would be able to set rules and teach their children appropriate online behaviour (Valcke, De Wever, Van Keer and Schellens, 2011).

Over the past three years, several schools in South Africa have adapted to a fully digital e-textbook system. Currently, more than 170 schools, and over 50 000 children, are using the EduBook e-textbook system developed by Edu X (pseudonym) – an educational technology consultancy located in Gauteng. In most of these schools, the use of the EduBook system is mandatory for both learners and teachers. Some research has already been done on the adoption of this system. Weilbach and Matthee (2015) focused on the problems experienced by teachers while implementing the EduBook system in their classrooms. Matthee, Hattingh and Weilbach (2017) noted the feelings of helplessness experienced by parents regarding the drastic move towards technology-enhanced education in these schools. Parents felt out of control because of their insufficient digital literacy levels, as well as their concern regarding their children's cyber safety. Edu X is aware of the concerns of parents regarding cyber safety and approached the researcher for ideas on how to empower schools to address the issue. The researchers envisaged an information system which can be used by schools, or Edu X, to prepare for implementation based on parents' digital literacy level, their level of cyber safety awareness, the children's ages and their information delivery preference (online content, parent meetings, printed documents, etc.).

This study's objective is to provide a Cyber Safety Information Framework to act as the basis for an information system to help parents manage the change to mobile learning, while minimising the negative impact on their children's privacy and safety. In addition, it will provide a value-added product for the service providers to deliver to their clients in conjunction with the service requested.

1.3 RESEARCH QUESTIONS

The study will help to answer the following detailed questions:

INTRODUCTION

Main Research Question:

How should a Cyber Safety Information Framework be formulated such that it is relevant to the needs and expectations of parents?

Sub Research Questions:

- What are the cyber safety threats of using mobile devices, especially for learning purposes?
- What is being done locally and internationally to make parents aware of cyber safety in schools and at home?
- What measures are being taken by schools in South Africa to inform parents about the cyber safety-related issues when implementing the use of mobile devices?
- How can the information's needs of parents be determined in the South African context regarding cyber safety awareness?
- How can existing cyber safety information be categorised to fulfil South African parents' needs?
- What would an instantiation of the framework look like?

1.4 PURPOSE OF THE STUDY

The purpose of this study is to define the elements of a Cyber Safety Information Framework for parents such that service providers and schools can implement appropriate awareness before, during and after the installation of digital learning services. This study will also help to offer service providers and schools a Cyber Safety Information Framework relevant to parents' needs. Based on this framework, information will be disseminated and used during campaigns such that parents can use it to assist them and their children in remaining safe on the internet.

A Cyber Safety Information Framework, instantiated in a design for an information system, will help service providers and principals of schools to raise parents' awareness of cyber safety issues possibly encountered online. Service providers provide tablets and/or mobile content, and by using such a system, service providers can give the parents suitable material as an additional service.

1.5 ASSUMPTIONS

Assumptions in research are things that are accepted as true. Assumptions should be stated to help the reader and the writer understand one another's viewpoints. If assumptions are out of control, the study may be rendered useless, especially in the area the research needs to be applied (Simon, 2011). As Leedy and Ormrod (2010) said, research does not exist without assumptions. This research will assume that the answers to the questionnaires will be honest and sincere and to the best of the participants' abilities.

- The results of the research will first apply to the specific parents who participated in the study, which could also be adapted and implemented on a larger scale.

In a South African context, the digital literacy levels and cyber safety awareness of parents vary extensively, and the framework could link these two factors in combining appropriate content.

- The school where the study takes place already has some form of cyber safety rules and policy. In a case there would not have been policies in place a step for the creation of policies should be added.
- The parents have children of the same age range.
- The analysis of the results is subject to the researcher's views.

1.6 SHORT DEFINITION OF MAIN TERMS AND CONCEPTS

Cybercitizen or netizen: a person that is a frequent user of the internet while being aware of the rights and responsibilities of taking part in the cyberspace (Ribble, 2015).

Cyber safety: wise and responsible use of the internet and technological devices like internet, tablets and cell phones (Australian Communications and Media Authority, 2010).

Cyber security: an ensemble of tools, procedures and guidelines that are established to safeguard networks, computers, programs and data from intrusions that may erase, change or damage them (Rouse, 2010).

INTRODUCTION

Awareness: consciousness or perception of a condition or circumstance (Dictionary.com, 2015).

Need: a lack of something (like information) requisite, desirable, or useful (Merriam Webster, 2019). What is defined as a need may differ from one population to the other.

Digital Literacy: Set of skills that include mostly the ability to use technology, get the most out of its opportunities and tackle the challenges involved (Gilster, 1997)

Digital Divide: a gap between technology accesses among the population (Dorner & Gorman, 2006)

Cyber safety threats: concerns and dangers regarding the safety of the users on the internet. The most common threats are cyberbullying, sexting, talking or meeting with strangers, accessing inappropriate content and being exposed to a breach of privacy (Beger & Sinha, 2012).

Framework: a research product which “explains, either graphically or in a narrative form, the main things to be studied. It describes the key concepts and the presumed relationships among them” (Miles & Huberman, 1994).

1.7 RESEARCH APPROACH

The research uses a Design Science Research Methodology approach, and at each step of the methodology, specific methods were used to complete the various steps of the process.

The Awareness and Suggestion phases of the Design Science Research Methodology uses a literature review as a method; the Development Phase mixes a literature review and a case study (using the qualitative and quantitative collection and analysis methods). The Evaluation phase is done by designing a prototype system, an instantiation of the framework and evaluating the system by getting feedback from intended users.

1.8 DISSERTATION LAYOUT

Table 1 below gives a short overview of the layout of the research.

Table 1 Dissertation Layout

Chapter	Summary
1	This chapter introduces the subject and its relevance to the industry. This chapter also gives the outline of the subject and highlights the research questions and the assumptions taken for this research.
2	This chapter is the review of the literature on the theme of the study: cyber safety awareness. It gives definitions of themes around cyber safety awareness and how these themes might be linked to the subject. It provides details about cyber safety itself, then relates it to parents. It also provides an overview of action taken, as well as related published frameworks.
3	This chapter emphasises the methodology used to achieve the goal of the study. It defines the Design Science Research Methodology used and motivates the reason why it was chosen for the research: This chapter will also describe in detail the way the chosen methodology had been applied throughout the research.
4	This chapter is a summary of the Awareness and Suggestion steps of the methodology used for the research, namely the Design Science Research Methodology. It forms part of the main cycle of the research. It summarises the reason why the chosen topic was relevant, and the valid gaps identified. This chapter also highlights the possible provisional solution to the limitations found in the topic, giving the potential components of the framework.
5	This chapter forms part of the Development of the methodology chosen in the research. It develops the Sub-Cycle 1 of the main cycle. It details the steps followed to create the Cyber Safety Information Needs Assessment Instrument.
6	This chapter forms part of the Development of the methodology chosen in the research. It develops the Sub-Cycle 2 of the main cycle. It details the steps followed to create the Categorisation of the Cyber Safety Information for Parents. This chapter also details the arrangements made to create the final version of the Cyber Safety Information Framework.
7	The evaluation of the Cyber Safety Information Framework takes place in that chapter. The framework proposed in the previous chapter has been instantiated through a system's design. This chapter reports on the evaluation by one possible user. It also reports on the refinement made to the framework, as well as the system design.
8	This chapter concludes the research. The final version of the Cyber Safety Information Framework and its instantiation will be shared with the public. It also reports on the contributions the study has made and the possible future studies.
9	This chapter comprises all the appendices referred to along the research.

1.9 SUMMARY

The prevalence of technology in communities is steadily increasing (Pollara, 2011), creating technology-savvy individuals who benefit from all the opportunities technology has to offer. The utilisation of technology, especially for learning purposes, should be accompanied by an awareness surrounding the users' safety. This awareness should involve all the participants; namely, learners, teachers, parents, school and government (de Lange & von Solms, 2012). The researchers realised in the introduction that most awareness campaigns were focused on learners only, and there was a lack of material available for South African parents, according to their specific needs. The researchers have also been approached by a service provider to emphasise the need for such material.

The next chapter will give an overview of the published literature around cyber safety awareness in South Africa, and around the world. This chapter will define the terms related to cyber safety, as well as the actions taken in this regard. It will also give examples of already published frameworks.

2 LITERATURE REVIEW

2.1 INTRODUCTION

This chapter will help to define some of the main concepts around cyber safety, as well as the potential risks that might be encountered, particularly from a South African perspective. The literature review will also discuss what has been proposed previously in other literature in accordance with reducing the risks facing mobile device users. The literature review will discuss studies and actions taken to increase parents' level of cyber safety awareness, as well as the previous frameworks published in the field.

2.2 DIGITAL CITIZENSHIP

A digital citizen is a person that uses information technology frequently to engage with the world around them. Mossberger, Tolbert and McNeal (2008) defined that a digital citizen possesses adequate skills, knowledge and an internet access point (which may be a computer, cell phone or a tablet) to interact with people from a distance. Digital citizenship might also be understood as a concept used by teachers and parents to help them gain awareness around what themselves and their learners or children need to know to use technology responsibly. It contributes to developing a universal understanding of the norms for the responsible use of technology (Ribble, 2015).

Ribble (2015) divided the concept into nine themes: digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness and digital security.

- *Digital access*: this discusses the fact that not all digital technologies are equal regarding the accessibility and the opportunities it creates. The goal of digital access should be to find a way to increase access to technology among populations. Helping to provide and expand technological access (as it will increase digital citizens' productivity) should be a primary concern.

- *Digital Commerce*: when technology may be used to buy or sell goods in remote locations. Users of the platforms (sellers and buyers) must be acutely aware of the issues possibly encountered in the online buying/ selling system they are using. Users should be taught about potential safety and security issues, how to be cautious and avoid problems that can be prevented.
- *Digital communication*: the fact that people can communicate with each other, regardless of their location. There are several ways of communication. Most of the time, people have not been taught how to choose between the communication options available.
- *Digital literacy*: as the world is evolving quickly, users must be able to learn how to use rising technologies efficiently and responsibly. Learners, parents, teachers and technology users need to be taught how to keep up with the latest developments.
- *Digital etiquette*: digital etiquette refers to norms of conduct and procedure for using information technologies. Digital citizens must be taught what the standards are to use technology appropriately.
- *Digital law*: as digital citizens are aware of the norms surrounding information technologies, these citizens should be accountable for any deliberate misuse of technology. It will make users more aware of their responsibilities and allow them to face the consequences of their actions.
- *Digital rights and responsibilities*: to ensure the safety of all users, some rights and responsibilities need to be outlined. For example, a digital citizen should know that one should not use technology to spy, bully or harm others. All digital citizens should also know that one would face legal consequences for their online actions. If one uses the internet for things such as stealing, child trafficking or compromising the country's peace, one will face severe legal actions.
- *Digital health and wellness*: there is a danger to the health and wellness of every technology user. Users should be made aware of all the risks involved in exposure and interaction with technology, as well as how to be protected from them.
- *Digital security*: there are wrongdoers and offenders who misuse technology and exploit users of technology. Digital citizens must be taught how to avoid potential security issues and how to stay safe and secure when engaging with technology and on digital platforms.

Raising the awareness of digital citizens on how to use technology responsibly should include the digital themes stated above (Ribble, 2015). From these themes, three global recommendations have come out. Learners and parents (users) need to be taught how first to *protect*, *educate* and then *respect* themselves and others while using the technology. In other words, users need to be aware of what is happening online and have a defined set of rules to follow.

The Digital Citizenship and Safety project was an initiative run by UNICEF in 2011. Their primary objective was to work with young adults in various countries in mastering new and traditional technologies to become productive members of society. Based on this project, a study was conducted in South Africa where UNICEF developed materials to increase the awareness of young people on responsible and safe usage of the internet and communication technologies. UNICEF concluded that South African organisations and the government are actively promoting online safety, but given the rapidly increasing number of digital citizens, there is a need for well-structured laws and education materials, especially new users (Beger & Sinha, 2012). In a study done in 2009, Hollingworth, Allen, Kuyok, Mansaray and Rose (2009) discovered that new digital citizens are mostly parents and teachers, as these new digital citizens are believed to be the “technology immigrant” generation who were born before the information technology era and are often reluctant to adapt to the evolution. Materials must be developed for them to cope with the current trends in technology such that parents and teachers can be an example for the younger generations.

2.3 CYBER ETHICS

As technology advances, new ethical dilemmas appear (Lynch, 1994). The use of technology involves the development of unique types of moral choices that society needs to be aware of and put into practice (Mason, 1995). The definition of cyber ethics draws on the traditional understanding of ethics: a set of regulations that became norms (Makinen & Naarmala, 2006). These regulations define what is considered as right or wrong within a population (Resnik, 2011). Cyberethics (also known as computer or internet ethics) help to identify the boundaries of acceptable behaviour while using technology. Moore (1985) also

emphasised the research to be done in this area, because multiple policies may arise out of the possibilities technology and computers offer. Further ethical and legal actions and decisions need to be applied with the introduction of new technologies, so as to find a balance between the needs and rights of everyone using the technology (Lynch, 1994).

Tavani (2004) defined cyber ethics as the field of ethics that inspect mostly legal issues, but also moral and social ones, that come with the improvement of technology. With cyber ethics, users are being told to recognise and practice ethical and legal rules when accessing, using and creating new technologies (Pruitt-Mentle, 2000). It establishes boundaries for each user so as not to harm themselves or others and assists in recognising online risks and counteracting them (Pruitt-Mentle, 2000). Cyberethics should be taught as a basis for cyber safety, primarily for users to be aware of potential consequences if the boundaries are breached.

The Internet Architecture Board (1989, p. 1) have considered the following activities as being unauthorised on the internet:

- searching for unauthorised access to resources on the internet
- abusing the main use of the internet
- wasting resources like capacity or devices
- destroying the integrity of computer-based information
- compromise the privacy of other users

These general guidelines could also serve as a starting point to define what cyber ethics mean in practice. It also helps to define a universal set of ethics that can be followed by everyone.

The education of cyber ethics for learners is often seen as primarily the responsibility of the parents (Pusey & Sadera, 2011). Lee (2010) mentions that many children discover and explore the internet and all its possibilities without any guidance or supervision from parents or teachers. Calluzzo and Cante (2004) also point out that most of the learners involved in their study had a misconception of what is considered right or wrong online behaviour. Hollingworth, et al. (2009) mention that even if some parents want to help their children,

parents may not possess adequate knowledge or power to supervise and guide their children. Some parents think that the internet their children are accessing via a computer is not the same as the internet accessed on a cell phone or tablet. Parents may believe that the web accessed on mobile phones is less disturbing than the one accessed via a computer (Bada & Sasse, 2014). Additionally, some uninformed parents believe their children may incur no risk when being online with them in the same room (Naidoo, Kritzingler and Look, (2014). Atkinson, Furnell and Phippen (2009) added that the lack of cyber safety awareness and cyber ethics of adult's results in an inability to teach the younger generation how to behave online. These misconceptions should be assessed and addressed before expecting parents to be part of their children's learning and socialising experience on the internet. Parents must empower themselves first before they can control what their children are doing online and teach them what behaviour is acceptable or not (Cole, 1999).

It is the direct responsibility of every parent, as well as the school, to instil an ethical code of conduct to learners (Sukhai, 2004). Parents and the schools must, therefore, cooperate. Unfortunately, parents often lack information about school policies regarding internet and technological devices (Kong & Li, 2008). Despite the fact that some schools do have such policies, research shows that learners, parents and sometimes even teachers are not aware of them (Bell, 2002). Being informed about these rules may help them to guide their children's use of the internet and technological devices. It is suggested that there is a need for an active collaboration between school and parents in working together towards children's cyber ethics awareness. Organising parent-child workshops or sharing documentation on a day-to-day basis with parents and children would be an efficient way to educate both parties (Kong, 2008). This will also help parents continue the cyber ethics education in their homes.

2.4 CYBER SECURITY

2.4.1 Cyber Security Overview

Keeping information secure is as old as information itself (Rusell & Gangemi, 1991). From the moment information started to be shared and transmitted, there was a need for it to be

secure, arriving at the intended receiver intact and understood by only him or her (Dlamini, Eloff and Eloff, 2008). Cyber security has different meanings. It may refer to the measures taken to protect information, computers and networks from unauthorised access, alteration and/or destruction as defined by Gallaher, Link and Rowe (2008). It involves technical interventions that protect hardware and data from unauthorised access and damage (Pusey & Sadera, 2011), included, but not limited to, the use of a password for protection, firewalls and anti-virus software. Cyber security also comprises security “safeguards, security concepts, risk management policies, guidelines, technologies such as antivirus software, actions like security campaigns and also training needed to allow information and hardware to remain secure” (Nambiro, Muchiri and Matoke, 2014).

In the early days of computers and technology, a security attack was not as severe as it is today. Security breaches were only viruses or worms that could make messages or images appear on the screen of the computers without causing any lasting damage (Dlamini, et al., 2008). Robert Morris created the first worm in 1988. Although it was not meant to be harmful, it created trouble amongst computer users at the time (Denning, 1991). As time passes and technology advances, cyber-attacks have drastically evolved and became more dangerous and sophisticated (Dlamini, et al., 2008). The internet and organisations, as well as the people's dependence on it, have offered criminals a new platform where they can spread and expand (Selwyn, 2008). It also makes crimes easier to commit because offenders can be anonymous and done from a distance, which means they could go unpunished (Hunton, 2011). Intruders are no longer only using worms and viruses but are also using more complex security attacks to get unauthorised information and damage data and hardware (de Joode, 2011). As a result, people and organisations using the internet for communication and financial transactions, are potentially at risk to have their personal and financial information compromised by individuals with malicious intentions. The use of new and updated types of interventions are required. Security is widening, to include not only technical interventions, but also risk management, information security management, as well as legal and regulatory compliance of all the technology's users (Volker, 2007). The challenge of keeping information secure has seen the emergence of new needs that require a multi-disciplinary, proactive and flexible approach to ensure overall cyber safety (Theoharidou, Kokolakis, Karyda and Kiountouzis, 2005).

2.4.2 Towards Raising Cyber Security Awareness

Raising security awareness and security education efforts must be coordinated with, and involve, governments, organisations, homes and schools (Dlamini, et al., 2008). Several developed countries have effectively implemented regulations, tools, protocols and standards to be applied for cyber security. To make it even more efficient, these countries run numerous campaigns to exhibit and educate the population and organisations about what is available and what everyone can do to build a secure cyber space (Kortjan & von Solms, 2013). For example, the UK government has invested six and a half million pounds to educate their population on cyber security and familiarise them with the concept and the various actions to be taken (Cabinet Office & The Rt Hon David Cameron MP, 2011).

South Africa, with other developing African countries (Nigeria, Cameroon and Ghana), ranks in the top ten countries in the world with the highest number of cyber-attacks (Akuta, Ong'oa and Jones, 2011). Within Africa, the issues that occur most often, according to Ogundeji (2014), are: disaster recovery resilience, data leakage/data loss, lack of fraud support, inadequate/inefficient identity and access management and lack of regular security testing. Kritzinger and von Solms (2012) attempted to explain this fact by identifying four major problems with cyber security in Africa. 1) The study found that there is a lack of research on cyber security in the African context, which is research about the issues that may be exclusively relevant to Africa. 2) In addition, Kritzinger and von Solms realised that there are not enough effective guidelines and legal policies that can be applied to Africa. 3) There is a lack of awareness and regulation. Not enough campaigns are initiated. 4) There is a lack of security measures, like up-to-date anti-virus software installed on people's computers. Many African organisations do not possess enough knowledge of the various cyber risks and attacks to help them react to, and combat, cyber-crime efficiently (Ogundeji, 2014). One reason for this might be the fact that some African countries have a low rate of ICT infrastructure implementation (Cole, Chetty, LaRosa, Reitta, Schmitt and Goodman, 2008). The cyber security risk is even higher because, in Africa, there is a severe lack of cyber security skills and awareness among technology users (Ogundeji, 2014). Numerous African countries have shown an interest in cyber security, but very few have taken real action. In

South Africa, for example, there is an absence of national cyber security policies and awareness campaigns organised by the government (Dlamini & Modise, 2012).

Cyber security awareness takes place through independent organisations which target a specific audience to create a global impact. For the countries who were proactive in cyber security awareness, they focused predominantly on cyber legislation (Cole, et al., 2008). It seems that even if these countries want to take action, they are not sure of what they should do to meet their actual needs with regards to cyber security. Africa does not have general technical security measures. Cole, et al. (2008) mention that Africa does not have clear initiatives about cyber security, and some other African countries have very vague definitions and actions around the cyber security concept. However, Africa needs appropriate and pertinent laws, policies and practices if Africans want to combat cybercrime efficiently (Akuta, et al., 2011). These laws and practices need to be understood and applied in all the African countries for a more widespread effect. All the countries, by location and according to their realities with regards to information and communication technology infrastructure's implementation, need to integrate their efforts concerning cyber security just as the SADC countries did (Vecchiatto, 2005). Furthermore, as the cyberspace is seen as an international space, international global laws need to be enforced (O'Connell, 2012), not only by military force, but by countermeasures and rules that are internationally applied. Military force will only be utilised if the cyber-attacks affect the entire country's security.

2.5 CYBER SAFETY

Cyber security and Cyber safety are often mistaken for being the same thing, but they are not. Cyber safety, also referred to as internet safety or e-safety, denotes the study of the actions taken by people to use the internet and technological devices (personal computers, notebooks, Kindles, tablets and cell phones) wisely and conscientiously (Pusey & Sadera, 2011). It teaches individuals how to conduct themselves from a behavioural point of view rather than a hardware point of view, as with cyber security. These actions, and good implementation of them, tend to protect one's personal information and image, minimise the impact of the internet and the threats associated with communication technology, and creates a safer online, and even offline, environment for everyone (iKEEPSAFE, 2016).

2.5.1 Cyber Safety Threats

Cyber safety helps to build awareness of the potential issues that users may come across while using the internet and communication devices. These problems are often referred to as cyber safety threats. These problems may be related as one could be used to carry out the others. von Solms and von Solms (2014) established four groups of threats: technology-related, content-related, harassment-related and the risk of exposing information. The technology-related threats include the malware, virus and hacking; the content-related threats are when the user is exposed to inappropriate or illicit content; the harassment-related threats include cyberbullying, cyberstalking and all forms of unwanted online contact; and the risk of exposing information threat involves sexting, being exposed to a breach of privacy or being caught sharing information through phishing.

The elements of the four groups will be discussed below in greater detail.

2.5.1.1 Technology-Related Threats

Malware: which is short for malicious software, is a software that has been created to damage or disable computers and computer systems, or steal, compromise or erase information (Christodorescu, et al., 2005). Malicious software can either be a virus, Trojan horse, spyware or worms. This software can be installed on laptops, desktops or even smartphones and tablets. Some ways of being infected include clicking on unknown online links from social media, downloading infected items (movies, songs, mobile applications), opening emails with harmful links or attachments or visiting untrustworthy websites (Bothma, 2015).

Virus: A computer virus is a common type of malicious software (malware). It enters a system by exploiting its weaknesses. It may be security weaknesses or human weaknesses. Virus are often created to discover the vulnerability of a system or to perform harmful actions (Bell, et al., 2004). When it has entered a system, and it is executed, it completes its task by replicating itself within a program by writing its own code in order to destroy the original

information (Stallings, 2012, p. 182). It can infect hard drives, boot sectors and files of data (Aycock, 2006).

The term virus is commonly used to refer to other types of malware like keylogger, spyware, ransomware, worms or adware because they all result in an infection of the computer, sometimes with stolen personal information. Viruses can be used to access personal information like stored credit card numbers or other personal information, or to collect pressed keystrokes, display specific messages or advertisements on computer screens, corrupt data, spam emails or even make the computer unusable (Ludwig, 1998).

Hackers - Hacking: the term hacker is commonly used to refer to an individual who gains, or attempts to gain, unauthorised access to computer systems or networks (Furnell & Warren, 1999). A hacker may hack for several reasons. It may be to evaluate the weaknesses of a system, to gather or alter information, to protest or to make an illicit profit (Winkler, 2005). Depending on the intention and results, the hacking will be considered legal or illegal. Hacking can cause a significant financial loss because of the nature of the information stolen or the loss of the hardware, as well as personal information loss or theft (Furnell & Warren, 1999).

2.5.1.2 Content-Related Threats

Age-inappropriate content: Youth may have unintentional access to inappropriate and harmful content (Australian Communications and Media Authority, 2015). It might appear while children accidentally, or voluntarily, access content, or while following unknown links, mistyping online search terms or communicating with strangers. It might sometimes be a result of man-in-the-middle attacks. Following unknown links may also lead to malware, adware or spyware infection. A US survey reported that 42% of teenagers surveyed had viewed pornography online, and more than 60 % of these exposures were unwanted by them. Coming across hateful speech or violence was the third most common issue online (Munro, 2011). Regrettably, there is a lack of research on the effect on children of involuntary access to inappropriate content (Munro, 2011).

Internet/ Technology Addiction: Internet addiction (commonly called problematic internet use) is the excessive use of the internet so much that it interferes with the daily life of an individual (Byun, et al., 2009). This fixation or compulsion may injure or cause distress to the person concerned, as well as their surroundings. Young (1999) has discovered five types of internet addictions that prevail among society:

- A cybersexual addiction, which is the compulsive use of adult websites
- Cyber-relationship addiction, which is the over-involvement of individuals in relationships that are happening online
- Net compulsion, which is obsessive online gambling, shopping or day-trading
- Information overload, which is when individuals compulsively surf the web or different databases.
- Computer addiction, which is obsessive computer-game playing.

Young (1999) realised that internet addiction had an impact on several areas of the lives of individuals. It causes familial problems, as it may decrease the time and desire to do household chores or be around family and loved ones, which may lead to tension and frustration. It can also cause academic problems in the sense that she noticed a decrease in class attendance and study frequency, as well as lower grades and the exclusion or probation from school due to the excessive use of internet at school or during lectures. It may trigger occupational problems in the work environment as employees, instead of performing their tasks, surf the internet, decreasing the company's productivity. That is the reason why several employers and schools are now monitoring the internet usage of their employees and students.

2.5.1.3 Harassment-Related Threats

Cyberbullying: This may be defined as the use of the internet and technological devices to harass, discriminate against and disclose of someone's personal information (Belsey, 2006) in the form of mean, false and vulgar comments with the intention of denigrating the person being attacked (Burton & Mutongwizo, 2009). It can be done anonymously or not, and affects mostly young adults (18-25 years old), children (Popovac & Leoschut, 2012) and primarily females (Pew Research Center, 2014). Cyberbullying may even be more dangerous than

traditional bullying (Boyd, et al., 2009). The main methods for cyberbullying are text messages, social networking, instant messaging, emails, pictures and video clips (Burton & Mutongwizo, 2009). Cyberbullying and online harassment are more widespread in some online environments than in others. The common environments where it can happen are: social networking platforms, comment sections of websites, online gaming platforms, personal email account and discussion websites (Pew Research Center, 2014). Unfortunately, because there is no standardised definition of cyberbullying, and because there are numerous different versions of cyberbullying (depending on population, age and background), adults, and even children, might have difficulties recognising it when it occurs. Sabella, Patchin and Hinduja, 2013). Kowalski, Limber and Agatston (2012) have tried to identify some variations of cyberbullying. They identified flaming, cyber harassment, denigration, impersonation, outing and trickery, exclusion and cyberstalking. Flaming is a small and angry exchange between two people on social media or a chat room. Cyber harassment is sending offensive messages repeatedly to someone. Denigration is the action of spreading false and degrading rumours about someone. Impersonation is taking someone else's identity to post hateful and misleading information on their behalf. With outing and trickery, the victims' private information is shared on the internet. Exclusion refers to a deliberate refusal or acceptance of the victim into a social network, to make people feel rejected from a group that he/she would like to be part of. In this case, **cyberstalking** means receiving/sending intimidating and aggressive messages repetitively. Badenhorst (2011) added outing, which is sharing personal, secret information about someone with people with whom the information was not intended to be shared. He also mentioned happy slapping, which refers to when someone walks up to someone else and slaps the person while a third individual records the scene using their phone's camera. The scene will later be posted on social media.

Cyberbullying can have devastating consequences. It may result in the bullied victim having low self-esteem, frustration, anger and even suicidal ideas or death (Patchin & Hinduja, 2011). It is paramount for caregivers, and children themselves, to be aware of these methods and their effects on people so that they can be avoided.

Sexting: It can be defined as the act of sending and receiving photos or videos where the individuals are naked or partially naked. It also includes sexually suggestive messages

transmitted through text messages or instant messaging (Burton & Mutongwizo, 2009). Sexting can also refer to the involvement of minors in sending and receiving nude content, which may also be classified as child pornography or paedophilia (Youth Online Safety Working Group, 2010). Sharing or keeping the suggestive content of minors constitutes an illegal offence as the law strongly prohibits sharing, holding or producing child pornography. The South African law prohibits sexting under the age of 16; it is seen as a criminal offence (Republic of South Africa, 2007). Usually keeping the “intimate” images of ourselves on our own devices is personal and is not an offence. The moment one decides to share this explicit content with another party, one should keep in mind that control is lost over what has been shared once it has been sent (Badenhorst, 2011). People might intercept the content before it reaches the recipients and the intended receiver may share it with unintended third parties. Children and parents must be conscious of these practices and what the legal consequences thereof are.

Sexting might often be carried out between two persons involved in a romantic relationship. When the relationship is over, one of the ex-partners may upload online the explicit content previously received by their former lover with the intention of humiliating or intimidating them (Citron & Franks, 2014). This form of abuse (often called revenge porn) has developed from sexting. Sexual images and portrayals are often shared on websites dedicated to this type of content, accompanied with personal information about the victims such as their personal addresses, workplaces and phone numbers in order for them to be easily reached by stalkers and predators (Bazelon, 2013). Revenge porn has been a phenomenon hard to define, and the consequences of such a practice have long been neglected (Citron & Franks, 2014). With the increasing occurrence of such practice and its implications, which could lead to the suicide of the victims in some cases, countries like the European Union countries, USA, Canada and Australia have enforced legislation to counter this problem (Greenfield, 2013). These measures state that all material where one appears have copyrights, and before sharing it, necessary written consent should be obtained by the party who wants to share the content. Governments have also adopted severe legal actions and punishments for revenge porn perpetrators in legislation.

Another relatively new kind of abuse called sextortion has risen from sexting. A serious crime which is becoming increasingly prevalent, especially among children. In April 2016, the US

Department of Justice declared it to be “by far the most significant growing threat to children, with more than 60 per cent of their survey respondents indicating this type of online enticement of minors was increasing” (US Department of Justice, 2016). It is perpetrated by a person or a group of individuals threatening to share private and sensitive material of other individuals if the victims do not provide sexual images or videos of themselves, sexual favours, or sometimes even money, to the perpetrators (The Federal Bureau of Investigation, 2015). Predators may also intimidate the victims by threatening to harm their family or friends if the victims do not cooperate. Perpetrators often pretend to be people they are not, with the intention of gaining young people's trust in chat rooms and not getting caught. Criminals can obtain private and sensitive material through the hacking of the victims' electronic devices or via the victim's private online conversations where they share or stream this kind of explicit content. Offenders often target children that are willing to chat with strangers in chat rooms and engage in live streaming video activities (Jackman, 2016). It is very common for investigators and forensics to find out that one single sextortion offender has been in contact with hundreds of potential victims and keeps organised folders of compromising information about them (US Department of Justice, 2016). Sextortion has devastating consequences on young people particularly. It can lead to emotional depression, their grades at school may decline and they could get involved in self-harming behaviours which might, in severe cases, result in the child's death (US Department of Justice, 2016), all because of their fear of being exposed to their family or friends.

Talking with strangers online and possibly meeting them offline: The cyberspace offers an opportunity for everyone to communicate and share ideas and knowledge freely without personally knowing each other (Beger & Sinha, 2012). Unfortunately, it provides a broad platform for ***predators*** as well. It has been reported that at any given time of the day, at least fifty thousand predators are online browsing for children to target (US Department of Justice, 2006). The Internet allows them to target their victims and communicate with them in several ways. It often occurs in chat rooms and instant messaging. Predators find children online and then try to find enough information about them on social media, and then pretend to be their friend and gain their trust. Predators often pretend to be younger than their actual age and to have the same interests as their victims. They aim to isolate their victim emotionally and physically to abuse them sexually (Crosson-Tower, 2005). This practice is referred to as child grooming. It may result in child trafficking and prostitution or child

pornography production (Levesque, 1999). Child grooming over the internet mostly occurs among children between the ages of 13-17 years old, with the majority of them being girls (Munro, 2011). Furthermore, Livingstone and Bober (2005) have reported in a survey they did in the UK, that a third of children between the ages of the 9-19 years old, who go online at least once a week, have experienced unwanted sexual (31%) or nasty (33%) comments via e-mail, instant messaging platforms or SMS. Unfortunately, only 7% of their parents or caregivers were aware that their child had received such comments. This substantiates that parents and caregivers are not aware of what is happening online with their children and should be given appropriate information to raise their awareness to do so.

In South Africa, it has been reported that an increasing number of young people are meeting strangers online and then meeting them in person (Chigona, et al., 2009). A significant number of youths confessed that the person met did not look anything like what they were expecting (von Solms, 2011). This a very alarming fact which parents need to be aware of, especially because most teenagers do things online they would not want their parents or caregivers to see (Lenhart, et al., 2005).

2.5.1.4 The Risk of Exposing Information

Sharing personal information: Social media comes with the ability to share personal information. There is an issue of the type and quantity of information shared online to remain safe while using technology. Youngsters are the most vulnerable as they generally do not know the type and amount of information that can be shared safely online. A Euro RSCG Worldwide (2015) study titled "This Digital Life" that surveyed internet users in 19 countries highlights the following facts.

Almost 40 per cent of internet users are between 18 and 35 years old. The respondents in this age group are also concerned with the fact that people in general share too much personal information on social media. Over half of the respondents are scared that friends or family will share more than they would give consent for about themselves on social media. The youth in this research emphasised that other young people are always quick to share anything and everything on social media without weighing the consequences.

There is a real concern about over-sharing personal information on social media because not only may it cause an embarrassment, it may also lower the chances of being employed or getting life policies, or make you a target of scammers and stalkers (WEROBOT, 2017).

Location Sharing: Location sharing technologies are applications or software that allow one to track and share individuals' location using GPS or other processes, and relay the information to either friends, family or advertisers (Tsai, et al., 2010). "Check-in" is a function used on social media whereby the user is able to share their current location with their network or to the public, depending on their account settings. On Facebook, for example, the account may be public. This means that if one searches on a search engine 'the name of a person + Facebook', their profile is going to appear along with all the information on it that is not private. Some users, especially youngsters, may find the location sharing feature very intelligent, not realising the terrific safety risks it might carry. It allows everybody, including predators, to trace the users' current moves and study the habits of their prey (Li, et al., 2018). Location sharing also raises the issue of **cyberstalking**.

Internet Fraud is the type of fraud that makes use of the internet. It comprises multiple kinds. It can go from email spams to online exploitation commonly called scams. The most common type is phishing, which is when a website or an email portrays a trustworthy entity and asks to enter personal information like credit card details, account details and profile credentials for malicious reasons (Ramzan, 2010).

Acronyms use: The use of acronyms to facilitate communication in shortening messages is an example of a language created by the online community (Huffaker, 2004). Children now make use of abbreviations on social media or chat rooms in order to escape the vigilance of their parents or guardian, or to check if they are talking with their peers (Huffaker, 2004). Children may use them in order to communicate quickly and easily which creates a trusting atmosphere. Acronyms may also have a sexual meaning that may be used by predators to interact with children (SAPS, n.d.). Parents or guardians need to be continuously informed about the meaning of these acronyms so that they can spot potentially alarming facts.

Breach of Privacy – Identity theft. This involves individuals who want to change their identities with malicious intentions. It also comprises people that are using others' names or images as if they were their own, or using people credentials without their permission. Identity theft is one of the fastest growing crimes worldwide (Social Security Administration, 2018) and often occurs without the victim knowing. By taking someone else's identity, one can obtain bank loans, get credit cards and live a high lifestyle all in another person's name. For it to happen, the thieves need to get personal information about the victims. This information is often collected through social media or hacking into someone's devices physically or through a network (Information and Communication Technology Services, 2013). In South Africa, identity theft is costing businesses an average of R1 billion a year. Targets are mostly men of 30 to 40 years old. The perpetrators are known as flickers and are rarely caught (Erasmus, 2015).

2.5.2 Cyber Safety Skills and Digital Literacy

Digital literacy refers to the skill set required to participate in the digital era. These skills are more than the ability to use digital devices, and also include "reading" instructions from graphical presentations in user interfaces; using digital reproduction to create original materials from existing ones while considering copyrights; constructing knowledge from a nonlinear, hypertextual navigation; assessing the quality and validity of information; and having a mature and realistic comprehension of the "rules" that prevail in the cyberspace" (Eshet-Alkalai, 2004). Although cyber safety skills and digital literacy are not synonymous, Sonck, Livingstone, Kuiper and de Haan (2011) show that they are carefully related. They found that amongst European children aged 9 – 16, those with high levels of digital literacy are also much more skilled in safely navigating online activities. Sonck et al. (2011) imply that enhanced digital literacy will consequently strengthen cyber safety skills and vice versa. Digital literacy empowers one to browse the internet safely, change privacy settings on platforms and devices, judge the quality and reliability of the information accessed and understand and apply the online norms (Telstra Corporation Limited, 2014) to make informed decisions.

South African teachers and parents do not have access to information and known policies to assist children (von Solms & von Solms, 2014) which results in a general lack of knowledge and skills from them about ICT and its challenges. At the same time, the majority of African countries, including South Africa, do not have initiatives for raising Cyber Safety awareness among children, parents and teachers (von Solms & von Solms, 2014). Additionally, in South Africa, the high level of digital illiteracy, in conjunction with low access to ICT infrastructures, the language barrier and the geographic location of individuals, have a substantial impact on cyber safety awareness (Kritzinger, 2015).

2.5.3 Parents, Teachers and Cyber Safety

Parents and teachers play a significant role in the cyber safety awareness and education of children and must work together towards it. For teachers, it is essential to know how to recognise and react to these issues in the school and home environments. It will help them find the language to assess, respond and report these kinds of sensitive issues (Hanewald, 2008). It will aid them in providing the appropriate support to the affected children.

For parents, it is essential to recognise these threats and react to them immediately to minimise the impact it may have on their children. Schools should be able to help raise parents' awareness of cyber safety for them to actively contribute to the cyber safety education of their children (de Lange & von Solms, 2012). Schools should be providing lessons and adapted material as part of their curriculum. Parents also need to experience the issues their children could encounter online for the awareness session to have a significant impact (Ktoridou, et al., 2012). It will assist parents in structuring discussions they should regularly be having with their children. These discussions would mostly be to sensitise kids about what they may encounter online. Suitable policies to adopt appropriate behaviour and raise awareness online need to be developed and shared with parents, children and teachers to prevent and respond to the occurrence of cyber safety threats (Hanewald, 2008).

In European countries, parents with lower levels of digital literacy have a tendency to be more restrained towards the usage of the internet by their children and could, therefore, be

restricting the learning and online exploration of their children. Those parents with higher levels of digital literacy tend to embrace technology with their children and guide them more effectively (Duerager & Livingstone, 2012). Duerager & Livingstone (2012) recommend that instead of restricting the internet usage of their children, parents need to embrace technology and enthusiastically be part of their children's online experience. Parents need to discuss the possible dangers with their children, engage with their children's internet use and set rules according to their children's age. Parents with lower digital literacy, from both developing and developed countries, will not be able to impose rules on their children concerning online behaviour, letting their kids discover the internet on their own. The parents that are more knowledgeable would be able to set rules and teach their children appropriate online behaviour (Valcke, et al., 2011).

2.5.4 Towards Raising Parents Cyber Safety Awareness

As the cyberspace is a global virtual space, its issues are also not bound to a specific territory. Some governments in Europe and America, for countries like the United Kingdom, the United States, Canada, Australia and New Zealand, have noticed the persistence of cyber safety threats, and in response to that, have allocated a part of their budget to awareness and education about the phenomenon (Hanewald, 2008). These engagements are crucial to reducing the prevalence and overall impact of these threats.

2.5.4.1 Campaigns in Developed Countries

In Australia, a great campaign about cyber safety is underway, as the government wants their population to enjoy the cyberspace with as few risks as possible. The government has created an interesting interactive website, which contains, for the parents, instructional videos and articles with general knowledge and how to assist children with cyber safety. It gives valuable information about the available parental control tools, and teaches them about what is trending among children like hashtags and social media. The site gives hints about applications their children might be using, and the risks associated with them. It also explains to parents the role they should play and how to treat the cyber safety issues according to the age of the children (see Figure 1).

LITERATURE REVIEW

Let's face it, the internet is an integral part of young people's lives. Used responsibly, the online environment is a great place for our children to socialise and maintain friendships, be entertained, download and watch music and movies, play games, to search for information and to learn.

The ever changing nature of the internet can pose challenges for parents who wish to keep on top of their children's technology use. While children might seem to be tech savvy, they still need a parent's guiding hand to help make sure their online experience is positive and safe.



The high level



Figure 1 High-Level Information Menu

By clicking on any of these coloured squares (see Figure 2), parents will receive an overview of safe practices and online risks. If parents need more information on a cyber threat, they can select it from a menu (see Figure 3).

LITERATURE REVIEW

Figure 2 Online Threats Menu



A detailed procedure produced in a printable format, and a direct link or useful contact to report each issue, is also provided (Australian Government, 2016) - see Figure 4.

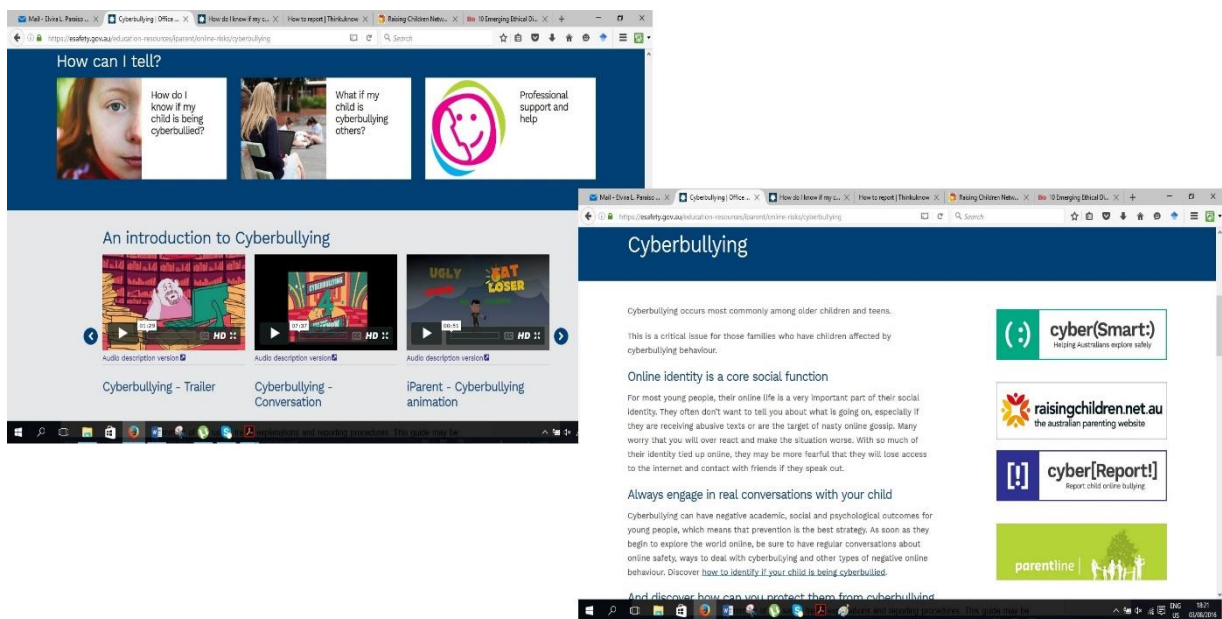


Figure 3 Cyberbullying Information on Esafety.gov.au

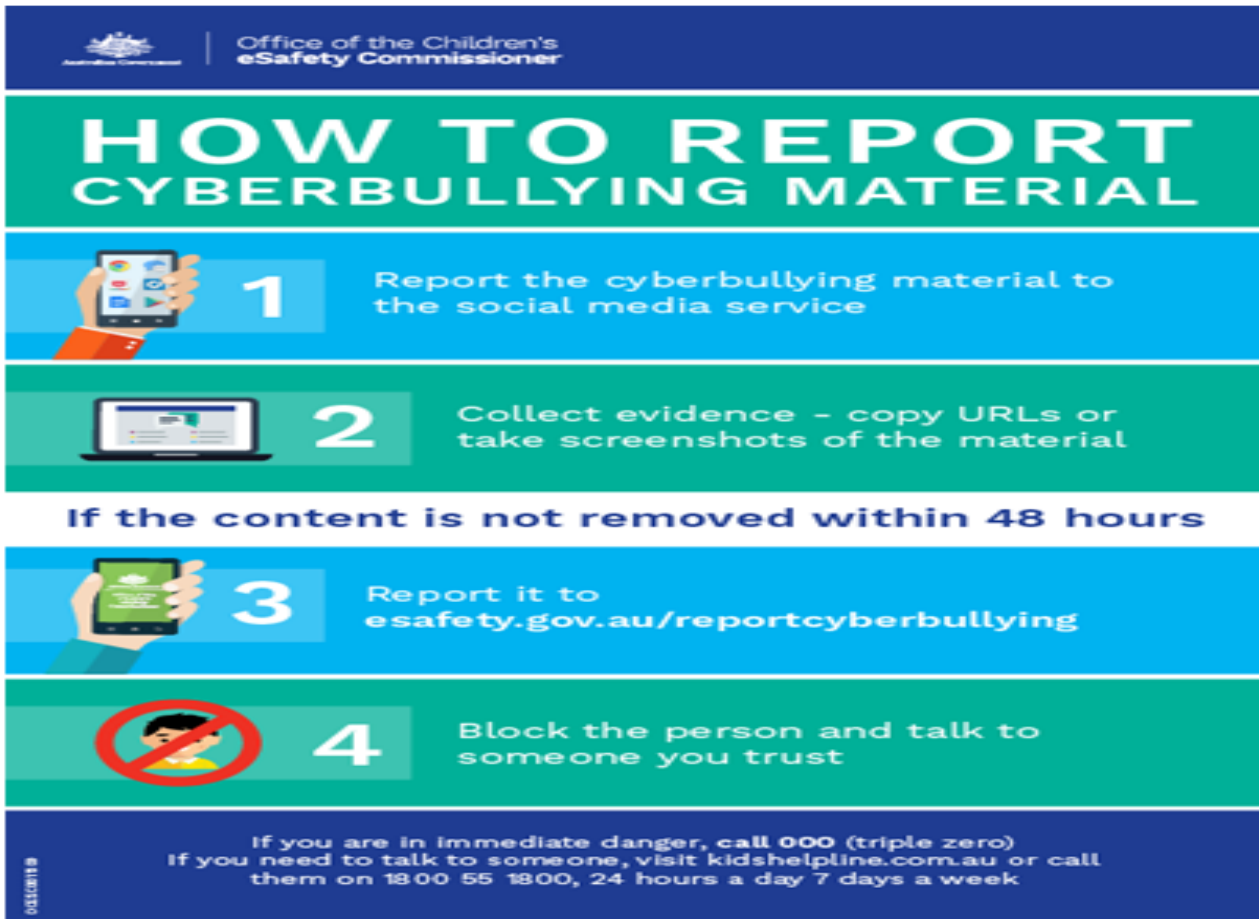


Figure 4 Procedures to Report Cyberbullying from Esafety.gov.au

The government believes that the material given to the parents should be simple and straightforward. Furthermore, parents should have access to concise and printable material that can be kept next to the computer area for everyone's awareness (See Figure 5).

On this page, parents can also download a pdf version of a guide for cyber safety. It is a summary of the safety threats explanations and procedures on how to report them efficiently. This manual is provided in several languages and may be printed and kept close by if needed.

In Australia as well, Parenting South Australia (a website that gives tips to parents about trending matter) have released an easy guide to cyber safety. It is a small online document which offers parents a summary of the issues their children could encounter. These threats are explained and details on how parents could detect and react to them are presented. The tips provided are very detailed and easy to understand. It also directs parents to websites

where they can have more extensive information about that specific issue and available contact numbers where they can report problems (see Figure 5) (SA Health, 2013).

Children and the online world

Parents today have seen technology grow at a rapid pace. New words such as Facebook, social media, apps and smartphones have become part of everyday language. Some parents are very familiar with new technologies and use them a lot. Some may use them a little, while other parents can think this 'new world' is not for them.

Whatever your views about online technology, it is important to realise it is very much part of children's 'real world'. It's where they can spend a lot of time and gain many educational and social benefits. As they get older, their online communication becomes a key part of their 'social identity'.

What parents can do

Parents often worry they don't know enough about online technology. That's OK – you don't have to be an expert. The most important thing is to be involved and not leave children to work it out on their own – just know how to find things out and where to get help. It might be easier than you think to become a 'digital parent'.

It is important to:

- > start early and talk with children about what they are doing. This builds trust. Children will accept your involvement in their online activities and

- > teach them to question what they see online and to realise not everything they see is real. You might ask 'Why do you think they are doing that?' or 'What would happen if they did that in real life?' This helps children learn your family values and to be critical consumers

Don't let the online world shape children's values – they need balanced information and guidance from you.

- > have rules and limits that suit each child's age and maturity – these will change as children grow up and gain skills
- > agree how you will filter and monitor internet use to make sure children are safe. Be upfront – if you go behind their back it may encourage them to hide things from you
- > make sure children have plenty of 'technology-free' time. Learning to entertain themselves without technology is a skill that needs practice. Active and creative play are important for children's healthy development. A balance of online and offline activities helps them develop a range of skills and interests.

It is important to stay involved in your child's online life. How you do this will change as children gain skills and become

Figure 5 Parents Guide to Online Safety (SA Health, 2013)

An American organisation called CyberAngels created a complementary cyber safety guide for parents in 1995 and was published in 2007 by the Association of Time Warner Cable. It gives the common uses of the internet by children in case some parents were not aware of all of them. The guide also contains explanations of various acronyms children might use in chats that parents are not supposed to understand. It then gives tips to parents on how to prevent cyber threats (See Figure 6) (CyberAngels; Time Warner Cable, 2007).

TALK TO YOUR CHILD ABOUT

Nicknames and Profiles
Avoid choosing provocative or identifiable nicknames. Keep personal information out of your online profile.

Receiving Files
If you are accepting files from someone you do not know, or even from a friend, be aware that files can carry a virus that may corrupt or delete data from your computer.

Strangers
Teach your child not to chat with online strangers.

Etiquette
Good etiquette should be used on the Internet as you would in person. While chatting, refrain from making comments that would be considered inappropriate or offensive in verbal conversation.

ACRONYMS PARENTS SHOULD KNOW:

AFK / BAK Away from keyboard/ Back at keyboard	MorF Male or female	F2F Face to face
121 One-to-one	SorG Straight or gay	WRN? What's your real name?
ASL? Age, sex, location?	LMIRL Let's meet in real life	WUF? Where are you from?
PA/ PAL/ POS/ P911 Parent alert/Parents are listening/ Parents over shoulder/ Parent alert	TDTM Talk dirty to me	53x Sex
NIFOC Naked in front of computer	ADR Address	Cyber Cybersex, sex over the computer
	WYCM? Will you call me?	WTGP Want to go private?

Figure 6 Example of Acronyms Used by Children from (CyberAngels; Time Warner Cable, 2007)

Canada and the United States have worked closely together to implement regulations and actions toward cyber safety and cyber security (Government of Canada, 2013).

The United Kingdom government has included a National Safer Day in their calendar. It takes place on the 9th of February. On their website (See Figure 7), the government documents action taken during this day each year to share awareness on the matter. The website provides content like videos for teens, made by teens, and factsheets about internet safety which can act as a starting point for a conversation between parents and children (UK Safer Internet Centre, 2016).

Safer Internet Day 2016 resources for parents and carers:



Parent Factsheet



Conversation Starters for Parents



Leaflet: Supporting Young People Online

Find out more about [how to keep your family safe online](#) with the UK Safer Internet Centre's four steps:

Figure 7 Parents Links to Useful Resources to Help with their Conversation with Children and Increase their Knowledge on the Matter (UK Safer Internet Centre, 2016)

2.5.4.2 Campaigns in Africa

The African continent, which is a collection of developing countries, appears to lack ICT infrastructure implementation and cyber safety awareness, despite a large number of youngsters who are active in the cyberspace (Dlamini, Taute and Radebe, 2011). According to von Solms and Von Solms (2014), no serious cyber safety awareness campaigns exist to guide these young people and enhance their awareness (von Solms & von Solms, 2014). In South Africa particularly, de Lange and von Solms (2012) identified a lack of cyber safety awareness and education. There are currently no national initiatives from the government concerning cyber safety awareness and education targeting school-aged children (Kortjan & von Solms, 2014). Moreover, there are no cyber safety-related topics included in the general curriculum of schools (Kritzinger & Padayachee, 2013).

The cyber safety awareness campaigns are mostly initiated by independent or private entities to a targeted audience to create a national outcome in the long run (Dlamini & Modise, 2012). African Social Programmes and Initiatives launched a private initiative called Internet Safety Campaign Africa in 2013, with the aim of sharing awareness on cyber safety in South Africa to create a safe online environment for everyone, (see Figure 8) (African Social Programmes and Initiatives, 2015).

LITERATURE REVIEW

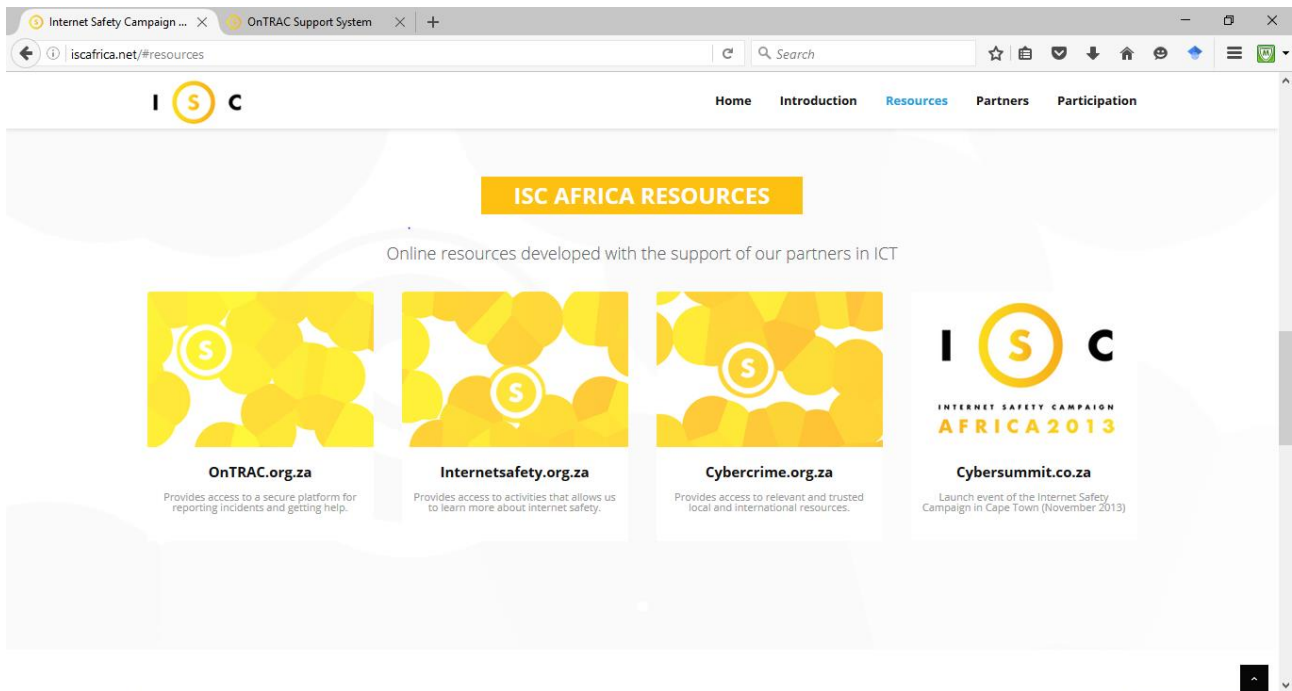


Figure 8 African Social Programmes and Initiatives – Home

The website is providing a platform where one can report threats and cybercrimes, and also receive assistance (OnTrac.org.za), resources with relevant and trustworthy links to websites with information that are pertinent to the South African Context (cybercrime.org.za) and resources to learn about internet safety (Internetsafety.org.za).

Online Technology Risk Advisory Council (OnTRAC) Support System provides a secure platform to report and track illegal activities happening online and obtaining advice on how to identify and react to online threat that everyone is a potential victim of (See Figure 9).

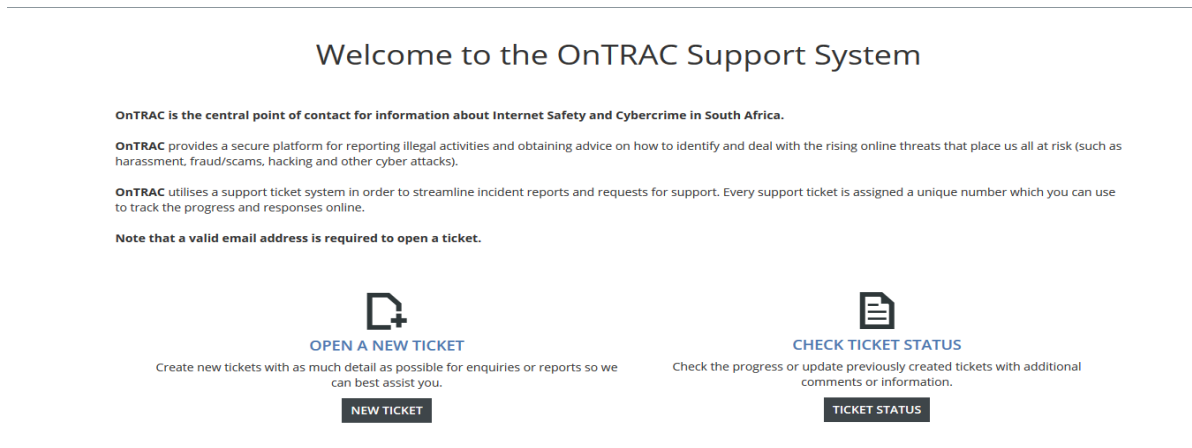


Figure 9 OnTRAC Support System

The Internet Safety Campaign promotes the Internet Safety Pledge, which outlines the commitments and fundamental principles that each person will follow as a supporter of Internet Safety. This website includes activities like a quiz where one can challenge their knowledge on right or wrong online decisions. The website also provides a teen's poll to understand their online experience and a parent's survey to understand their needs (see Figure 10).


Quiz on Internet Safety

Question 1 of 5

1 points

A few of your friends have been leaving mean comments online about someone you know. What do you do?

1. Join in – they're only having a laugh!
2. Report the comments to the website administrator
3. Support the person being targeted
4. Tell someone
5. Do nothing

 **Parent Poll**

Mobile Monitoring

- I don't use parental control tools on my children's cell phones.
- I haven't placed any limitations on my children's cell phone usage.
- I don't monitor the cell phone bill to see how my children use their time/data.
- I'm not sure how to keep tabs on my children's cell phone use without seeming intrusive.

Figure 10 Quiz on Internet Safety; internetsafety.org.za/quiz/

The cybercrime initiative, via the cybercrime.org.za website, provides an awareness portal intended for informational purposes. The website provides access to relevant and trusted local and international resources aimed at educating individuals at all skill levels about cybercrime and internet safety definitions and measures. The website also features help for reporting suspicious activities.

The South African Cyber Security Academic Alliance (SACSAA), an alliance of university research groups, also has a website where they share information about trending threats and practices around cyber safety and security. SACSAA also performs school visits upon request to share awareness of these topics (South African Cyber Security Academic Alliance, 2016). The South African Police Service (SAPS) offers a line to report cybercrime and cyber-safety threats, and on their website, SAPS give a short overview of what parents and children should know about cyber safety (SAPS, n.d.).

The African Centre of Excellence for Information Ethics (ACEIE), from the University of Pretoria, developed a toolkit for digital wellness in 2015 (African Centre of Excellence for Information Ethics, 2015). This toolkit consists of nine books compiled to promote information ethics in schools and communities in Africa.

- Book One: Digital Wellness Programme – Manual for workshop facilitator.
- Book Two: Digital Wellness Programme – Activity book for workshop participants
- Book Three: Digital Wellness Programme – Resource and concepts book
- Book Four: Digital Wellness Programme – Secondary school teacher’s manual
- Book Five: Digital Wellness Programme – Activity book for secondary school learners
- Book Six: Digital Wellness Programme – Primary school teacher’s manual
- Book Seven: Digital Wellness Programme – Activity book for parents of primary school learner
- Book Eight: Digital Wellness Programme – A roadmap for the campus community
- Book Nine: Digital Wellnests: Let us play in safe nests!

These books target different kinds of audiences in order to reach a higher number of people. It goes from primary school to university and filters through to the general community as well. It has been compiled to provide information and create activities to learn while interacting. There is a manual for the facilitator and the targeted audience in order for them to have similar information. In the case of children in primary school, there is also a manual for their parents in order for them to be aligned with the information given to their children, too.

The school or individual teachers may sometimes add a cyber-safety awareness programme as a topic to be taught. This uncoordinated state of raising cyber safety awareness among entities and organisations might be the reason for South Africa being third in the ranking of countries with the highest number of cybercrime victims (Symantec, 2013). There is a need for clear guiding principles and laws. Cyber safety materials should be drawn up in the 11 official South African languages, as children would appreciate and respond better to being taught about cyber safety awareness in their home language (Jobi & Kritzinger, 2014). Apart from being advantageous to children, it will also benefit teachers and parents, as it will enhance their understanding of the topics covered. Parents must

access cyber safety documentation to become familiar with the latest technologies their children are using. Parents should also be aware of what is trending among the youngsters, as well as the meaning of acronyms and jargon youth might be using. Parents should refrain from allowing their children to utilize social networking before the age of 13. In addition, parents should keep an eye on their children's activities to make sure they are safe (Faccio, et al., 2014). Parents can take advantage of the different software available, firewalls, history checking and browser's settings.

The type and efficiency of the measures taken by South African schools depend mainly on the budget and interest the school has put into cyber safety awareness, as there is no government policy or rule which force them to do so (von Solms & von Solms, 2015).

2.6 CYBER SAFETY FRAMEWORKS

The following paragraphs detail published frameworks for cyber safety and cyber security. Frameworks for cyber security have also been included, and the same principles found in these frameworks can be applied to cyber safety awareness.

2.6.1 A Framework for Cyber Security in Africa

This framework (Kritzinger and von Solms, 2012) was initially proposed for cyber security, but the same principles could be applied to create a safer online environment as well. The authors identified four imperative dimensions for efficient cyber security protection. These dimensions are briefly discussed below.

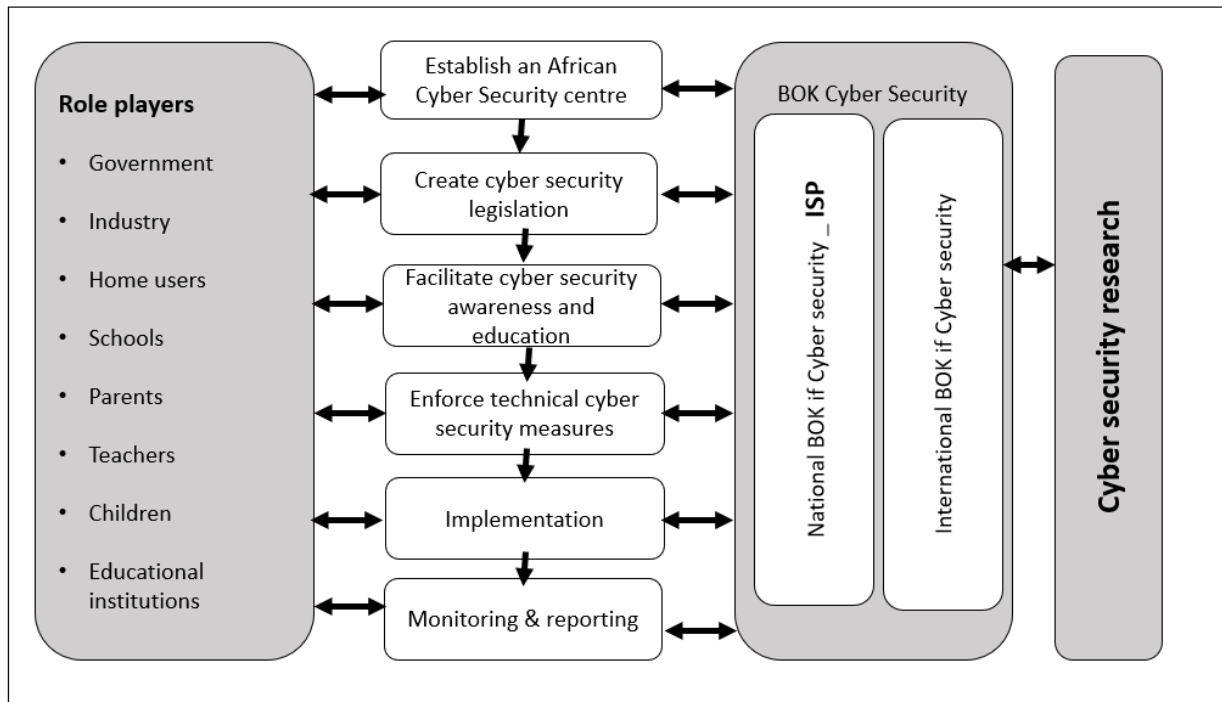


Figure 11 Proposed Comprehensive Framework for Cyber Safety by Kritzinger and von Solms (2012)

The first dimension includes all the **Role Players** that have a responsibility for the cyber security of the cyber users. Role players need to be identified, and each one of them should be aware of the specific role they play in the process. The role players include government, schoolteachers, parents and children themselves.

The second dimension is the **Body of Knowledge (BOK)**. It is essential that a BOK accumulated internationally be considered, as well as one that is unique to the realities of the location where the cyber security campaign is initiated. The Body of Knowledge refers to what has been locally or internationally published on a topic.

The third dimension is the **Cyber Security Research**. All the sectors involved should commit to doing more research to enhance the understanding of the context where cyber security will be applied and their different issues to provide more suitable and relevant solutions.

The fourth dimension is the **Cyber Security Actions**, the most essential of the entire framework. This fourth dimension comprises all the actions that need to be taken by all the

role players identified to ensure a safer cyberspace. These measures consist of, but are not limited to, creating global cybersecurity legislation, designing relevant cybersecurity awareness programs and monitoring and reporting of cybersecurity threats.

2.6.2 National Safe Schools Framework

The Standing Council of Education and Early Childhood of Australia (2010) suggested the following framework to guide the implementation of a safe environment for all. Although it refers to general safety, it provides useful components applicable to cyber safety as well. The framework identified nine key elements which need to be considered to assist schools in planning, implementing and maintaining a safe, supportive and protective learning community that enhance learners' safety and well-being. These key elements were based on published literature, good practice and feedbacks from educational systems, sectors and educators. The nine key elements are discussed below:

1. *Leadership commitment to a safe school*

It implies that all the members of the school should accept responsibility for the development and maintenance of a safe school. Members must also be aware of the rights and responsibilities they have in the matter. Schools and teachers must work together with parents to develop policies and rules for a safe environment, and the school must make sure that everyone is aware of the content of the policies.

2. *A supportive and connected school culture*

This component indicates that everyone should be connected and support the environment extolled by the school. Parents and caregivers should be involved in school activities. There should be explicit support and respect for everybody's beliefs and origins in the school. Also, there should be a wide focus on staff wellbeing; the school should make sure kids are respected and protected. Schools should provide monitoring and responses to child protection issues, too.

3. *Policies and procedures*

The school should compile clear safety policies and allow all parents, staff, and children to report any problems that one may encounter with ease. The school should,

furthermore, ensure that all the participants know the policies and regularly assess whether they are being upheld. The school should keep accurate records of any issues faced in order to be able to evaluate their occurrence and the quality of their own reactions and mitigation actions.

4. Professional learning

Parents and staff should be updated about the changes and trends in practice. Staff/parents should often be evaluated on their knowledge and skills for recognising and reacting to any issues relating to children.

5. Positive behaviour management

Children should always be rewarded and encouraged for their good behaviours and positive actions and choices.

6. Engagement, skill development and safe school curriculum

Schools should teach emotional and social skills to all participants. Participants should be able to listen competently, share openly with one another and advise wisely when needed.

7. A focus on student wellbeing and student ownership

Activities at home and school should always allow children to be in charge and handle the consequences of their actions, whether their actions are right or wrong.

8. Early intervention and targeted support

Effective procedures for early detection of issues among children should be compiled and shared with parents and teachers and updated when need be. Assistance for affected children should also be arranged.

9. Partnerships with families and community

Schools should work with the community to extend support to parents and children when needed and assist parents and caregivers by providing materials and training to educate them on the safety and well-being of their children.

2.6.3 Framework for an African Policy towards Creating Cyber Security Awareness

This framework was initially proposed for cybersecurity awareness, but the same principles can be applied to cyber safety awareness. Dlamini, Taute, and Radebe (2011) suggested this framework to provide guidelines for a cybersecurity awareness campaign. From their study, the parameters discussed below arose.



Figure 12 Cyber Security Awareness Framework proposed by Dlamini, Taute and Radebe (2011)

- **Identify the Intended Audience**
Select among all the roles players the one on whom the programme will be concentrated on
- **Define Topics to be covered**
Determine which topics usually covered by cyber safety should be emphasised during the sessions.
- **Establish Security Policy**

This part would be to define what are the rules and policies in place and who is responsible for compiling and sharing them.

- ***Define Delivery Methods to be used***

From the body of knowledge, several ways of delivery would have been gathered. At this point, it is a matter of deciding which way would be the most appropriate for the current audience. Dlamini et al. (2011) emphasised two sides in their case: employees and learners, and each method identified is adapted to the audience. For employees, the study proposed to use the emailing system, company newsletter or seminars/meetings, and for learners it proposed cyber safety posters and drawings.

- ***Develop a Strategy for Implementation***

A strategy to reach the audience will be established according to the requirements and the scale of the project.

- ***Design Awareness Strategy***

At this point the detailed design of the strategy will be arranged. The researchers will need to find out things that can be done to keep the audience interested during the entire session.

- ***Design Training Strategy***

This part includes the arrangement of the venue and the trainers, if needed.

- ***Develop Evaluation Methods***

This step suggests that there should be a way of evaluating or quantifying the impact and effectiveness of the training given.

2.6.4 High-Level e-Safety Framework

De Lange and von Solms (2012) proposed a high-level cyber safety framework to guide the implementation of cyber safety education in school. It comprises five components which need to be taken into consideration for effective cyber safety education in schools. The components presented in Figure 14 are discussed briefly below.



Figure 13 High-Level e-Safety Framework, de Lange & von Solms (2012)

Governance: The CONTROL Factor

This part implies that when starting any cyber-safety awareness initiative, cyber safety policies and school rules must be developed and implemented. These policies must consider covering ICT implementation in the school in general. The rules should be flexible enough to meet diverse aspects like internet access at school, the devices used and whether these devices are owned by the school or by the learners. Policies should clearly state inappropriate behaviours and their possible consequences. For these policies and rules to be effective, all the parties involved should be aware of them and the part they play in their application. A supervision and monitoring strategy should also be prepared and applied.

Role Players: The WHO Factor

As stated earlier, all stakeholders involved in a cyber safety implementation process should be identified. Each stakeholder should know precisely the role they need to play in the process and be willing to work together with the other stakeholders to implement effectively. The researchers have identified four role players, as discussed below.

- **The School**, which is seen as the entity that is responsible for developing school policies and rules. While doing so, the school must take into consideration legislation and regulations, and must also assume the accountability and lead the implementation of the cyber safety strategies. The school should appoint a person with enough cyber safety knowledge and expertise to coordinate the operations to facilitate this process, if possible.
- **The Teachers** can take on four different roles: *learners*, *advisors*, *teachers* and *identifiers*. Because teachers have to be able to recognise and respond to cyber-safety threats, the teachers need to receive training to prepare them. In this case, they will be seen as *learners*. Moreover, if children experience online threats and require someone to talk to, teachers need to be ready to listen and give advice. Therefore, they can also be seen as *advisors*. Teachers should be able to deliver consistent and efficient information about cyber safety to the children and will, therefore, play the *teacher* role. Teachers must also be *identifiers* and determine any change in children's behaviour or any disturbing facts that might need to be investigated.
- **The Parents** must play a significant role in raising cyber safety awareness of children. As it has been observed that parents are unprepared for cyber safety education, the parents need to receive the necessary training. In this case, they will be seen as *learners*. Following acquiring enough knowledge, they will become *teachers* as they will be required to educate their children. Similarly to the teachers, they must also be equipped to become *identifiers* and *advisors*, whenever it would be necessary.
- **The Learners'** needs should be determined according to their age, level of expertise and comprehension potential. The cyber safety education needs to be given from a very young age to develop the cyber safety culture. Learners, as for teachers and parents, can be seen as *teachers* who spread their knowledge to their peers, *identifiers* who

detect and report any disturbing fact to adults and *advisors* who help their peers when required.

E-Safety Topics: The WHAT Factor

Schools need to identify which topics of cyber safety need to be discussed and to what extent with each role player. Each role player needs to be directed to the place where one can find content adapted to their specific needs.

De Lange and von Solms identify essential topics to be covered as the advantages and disadvantages of the use of ICT, practical examples of how to handle different situations online and how to develop risk-awareness skills.

Resources: The WHERE Factor

These are the actual places where an individual can find information about cyber safety. Resources can be internal, as in from the school or teachers' initiative, or external resources retrieved online or at the library from existing published content.

External sources include e-safety websites or games and internal sources are e-safety videos, activities cards, teachable instructions, presentations, newsletter, leaflets, circulating letters or flyers. External sources may be used to compile the right internal sources for each participant.

Delivery: The WHEN Factor

This is the time when alternative lessons need to be implemented into the school schedule when a dedicated class cannot be accommodated.

Children found that the best moment was in the classroom, especially during the Life Orientation or Computer Application Technology classes.

For teachers, training workshops should be set up workshops.

For parents, awareness days, workshops or parents' meetings are most effective.

2.7 DISSEMINATING FORMATS AND CONTENTS FOR CYBER SAFETY AWARENESS CAMPAIGNS

According to de Lange and von Solms (2012), several formats that may be used to share awareness exist: Presentations, websites, videos, interactive content (games, quizzes, and activity cards), books, newsletters, hand-outs (leaflets, flyers). These formats will be discussed below.

Presentation

Teachers or trainers can make use of the presentation format using PowerPoint to compile information to be shown to the audience during an awareness session. The presentation will be used to support and demonstrate everything that will be said during the meeting. Elements in the presentation can be taken from the external and internal sources stated earlier, and their combination is adapted for each participant.

Websites

In some parts of the world, governments, the private sector and schools are trying to work towards people's (mostly children's) cyber safety. All the parties involved realised that it should be starting at home, and to do so, parents must be aware of what is happening and how they can assist their children. Governments in Europe and America created websites where people of all ages, including parents, could get information about the cyberspace and dangers one might encounter. This has been referred to in section 2.5.4. Most websites are divided into sections according to their visitors' status: parents, teachers or children, and children could be further divided into age groups, as each age group has their own information needs. Figure 14 shows that websites are providing content according to the audience that might visit their site, which can be parents, educators, government (law enforcement) or children (kids, tweens, teens).



Figure 14 Menu According to Intended Audience (US National Center for Missing & Exploited Children, 2016)

Share these tips, films and activities with your children:



Take the Quiz

Take the Safer Internet Day 2016 Quiz to find out if you make kind choices online.



SID TV

Check out films created for Safer Internet Day TV 2016.



Under-11s

Tips and films for under-11s for Safer Internet Day 2016.



11-18s

Tips and films for 11-18s for Safer Internet Day 2016.

Figure 15 Menu According to the Age of Children (UK Safer Internet Centre, 2016)

Videos/Films

Depending on the dissemination formats, there is a significant number of resources available for parents to enhance their cyber safety awareness.

Von Solms and von Solms (2014) have contributed to the body of knowledge by categorising 47 available videos according to the age of the children and their specific cyber safety information needs. A primary school teacher was used to determine the suitability of the videos for age groups and the typical classroom in an African school. Von Solms and von Solms chose to focus on Open Educational Resources (OER) because they can help African schools and houses with limited infrastructure to access quality content. OER are advantageous because they are free. No budget needs to be organised to access the material, OER do not require the creation of a specific account to access their content, and the content, which covers a vast range of subjects, is adapted to age ranges and is kept up to date. When searching for valuable content, one needs to take these previously stated criteria into consideration.

Content should be divided by the age of target groups as well as by the levels of digital literacy (von Solms & von Solms, 2014). It will ensure that parents receive content adapted to the age of their children. The formats of the resources shared need to be carefully chosen according to the audience.

Interactive content

The interactive content that the research of de Lange and von Solms (2012) referred to comprises games, quizzes or activity cards.

Games and quizzes can be found online and be used as external resources to increase the awareness of children and parents (Dooley, et al., 2009) and may enhance their learning experience. Games and quizzes can be found on websites highlighted in section 2.5.4 of this research.

The teachers or trainers, according to the audience and to make the activities relevant, may do the activity cards. The cards may be given during the awareness sessions.

Books

Books about Cyber Safety, targeting different audiences, can be found online on websites like Amazon.com or at the library. Books can be used in classrooms for more in-depth

courses or for children of parents who are not technologically-inclined. Some can be acquired at a fee, but free ones are also available. Some examples of books include: “Digital Wellness Programme - ACTIVITY BOOKS FOR SECONDARY SCHOOL LEARNERS” written by Bothma, T. (2015) under the University of Pretoria’s Information Ethics department, “Screenwise: Helping Kids Thrive (and Survive) in Their Digital World” of Devorah Heitner (2016); “Media Moms & Digital Dads: A Fact-Not-Fear Approach to Parenting in the Digital Age” of Yalda Uhls (2015); “Parenting in the Digital World: A Step-by-Step Guide to Internet Safety” of (Cranford, 2015); “Right Click: Parenting Your Teenager in A Digital Media World” of (Bamford, et al., 2015); “The Ultimate Guide to Internet Safety” of (Roddel & V., 2011).

Handouts

The teachers or trainers can take information from both internal and external sources in order to compile leaflets and flyers to be shared at school or during awareness sessions. Because handouts are concise, information will be straight to the point and easy to understand.

Newsletter

The school or organisation can provide a newsletter that parents or participants can subscribe to in order to receive targeted and frequently updated information about cyber safety awareness.

2.8 CONCLUSION

The chapter above has aided in defining some crucial terms regarding cyber safety and cyber safety awareness. Furthermore, it has reviewed what other scholars are saying about cyber safety, and the current role of parents and their involvement in their children’s cyber safety education. This review of the literature indicated that parents need to be a part of their children’s’ cyber safety education, but parents do not always possess enough knowledge and material to do so, especially in African countries. In response to this problem, this research will aim to produce a Cyber Safety Information Framework to educate South African parents. From the above literature, it is clear that the content should be appropriate

LITERATURE REVIEW

for the age of the parents' children and the way of dissemination should consider the level of digital literacy of the parent. The following chapter explains the methodology that will be followed to construct such a framework.

3 METHODOLOGY

3.1 INTRODUCTION

The research methodology details and motivates how the study has been conducted with the intention of solving the research questions and meeting the research objectives (Davison, 1998).

This chapter describes and motivates the methodology chosen to pursue the research. The research approach used is a Design Science approach, and sets out to answer the main research question: “How should a Cyber Safety Information Framework be formulated such that it is relevant to the needs and expectations of parents?”

3.2 RESEARCH DESIGN

A plan needs to be established beforehand to conduct a study successfully. This plan is referred to as the research design. The research design helps the researcher plan and actualise a study that is most likely to reach the intended aim (Burns & Grove, 2009).

The following sections will outline the design used to conduct the study.

3.2.1 Research Paradigm

A paradigm is a way of doing things, a set of theories and practices agreed upon by scientists of a common field. Guba and Lincoln (1994) defined a paradigm as a set of beliefs or worldviews that direct the actions and investigations performed in a research. Using a paradigm helps to illustrate how a problem should be understood and addressed (Kuhn, 1962). Information Technology (IT) and Information Systems (IS) research tend to be governed by particular paradigms such as positivism, interpretivism, critical and Design Science, to cite a few.

METHODOLOGY

According to Guba (1990) , a research paradigm can be defined by three characteristics: their ontology, their epistemology and their methodology. The ontology refers to what is the reality, the epistemology to how to acquire knowledge, know reality and provide justification of truth and belief. The methodology refers to the procedures used to gain knowledge. In IS and IT research, in addition to the three characteristics from Guba (1990), a fourth characteristic is commonly used: axiology. Axiology refers to the role of values in the research and the researcher's position in the research (Wahyuni, 2012) (Mouton, 2001). It is paramount to have an in-depth knowledge of these four characteristics when planning academic research, as these characteristics lead the kinds of assumptions, beliefs, norms and values of each paradigm one might use (Kivunja & Kuyini, 2017).

Using the guidelines and characteristics of Guba (1990), Wahyuni (2012) and Mouton (2001), four paradigms are discussed below.

- *Positivism* can be characterised as the fact that there is a reality out there ontologically. Epistemologically, because there is a reality out there, one needs to focus on reliable tools to discover the reality. In positivism, the researcher is independent of the data collected and maintains an objective position. The principal methodologies used are quantitative research approaches like experimental and survey research.
- *Interpretivism* can be characterised ontologically by the fact that there is no single truth because humans define what truth and reality are. Therefore, epistemologically, reality needs to be explained and interpreted according to events and humans' activities. The researcher is part of what is being researched and has a subjective position in the research. The methodologies used in interpretivism are qualitative approaches like action research or grounded theory, to cite a few.
- *Critical research* can be characterised by the fact that realities are socially constructed entities and realities are under constant internal and external influence, ontologically. Epistemologically, associations within the society should influence not only reality, but also knowledge. Critical research involves action research, ideology and critique as methodologies.
- *Design Science* can be characterised ontologically as that the reality belongs to a specific context so that reality may be multiplied. Epistemologically, reality, knowledge and truth are discovered through the creation of the artefact. Even though the researcher is active

in the creation of the truth, she is also trying to remain objective, especially in the evaluation. The methodologies used may be developmental like case study or prototyping.

The place for Design Science is under continuous argument. In the early 90's, there was an agreement about how to differentiate Design Science research from other paradigms (Peffer, Tuunanen, Rothenberger and Chatterjee, 2007). Hevner, March, Park and Ram, (2004) are of the opinion that Design Science is another paradigm that complements the positivist and interpretivist paradigm to research in the Information Systems field. The interpretive paradigm is widely accepted in Information System studies, but the result of the research could still be argued and contested (Peffer, et al., 2007) as the goal of interpretive research is said to enhance people's comprehension of their actions (Chua, 1986) and is mostly not applicable to the problem encountered in practice and research (Peffer, et al., 2007). However, Ivori and Venable (2009), sees Design Science research as based on both interpretivism and positivism and not as a separate paradigm besides positivism and interpretivism. Design Science paradigm has more or less positivism and interpretivism assumptions. This implies that interpretivism or positivism can guide the research and what needs to be achieved with the created artefact.

Several academic studies have accepted Design Science as a research paradigm, such as vom Brocke & Buddendick (2006) and Gregor & Hevner (2013) . This research also accepts Design Science as a paradigm with a specific methodology to use the paradigm and achieve our goal. This will be explained in the next section.

3.2.2 Design Science Research

Design Science Research was used to conduct this research. Conducting Design Science research in the Information Systems field provides evidence of the relevance of the Information System field to practice in the industry (Venable, 2006). Design Science research involves the conception of an innovative understanding of reality or truth by creating an artefact, and the evaluation of such artefact by the intended users to improve a given situation in Information Systems (Vaishnavi & Kuechler, 2004). Using Design Science

research helps to create products that are fully usable by humans, as well as profitable for them (March & Smith, 1995). Design Science research also supports inventing new methods and practices by creating original knowledge and insights. The researcher during this process is involved in multiple contextual situations, which force him/her to gain knowledge in the construction and accepts that the context affects the process and sometimes the results (Gilliland, 2014). Design Science must provide the evidence that the created artefact meets the purpose for why it had been built. If possible, proof that the resulting artefact meets the intended purposes even better than the artefacts previously created, could also be brought forward (Venable, 2011). The end-product of Design Science helps to bridge the gap between the current state-of-art and an ideal state-of-art (Hevner, et al., 2004).

In the context of the research, ontologically the ideal situation would be that everyone, especially parents, is cyber-aware. Parents should know to recognise and mitigate the risks of the internet and technology. However, in this context, the researchers realise that it was not the case. Epistemologically, the researchers used two sub-cycles in the development to gain knowledge and develop the artefact. The researcher was involved in the construction of the artefacts but tried to remain fair in the analysis and evaluation results. Qualitative and quantitative methods were used in the development process.

The following sections will give more details on Design Science research and how it was applied in this research.

3.2.3 Design Science Research Guidelines

Hevner et al. (2004) proposed a set of guidelines, which is meant to aid IS researchers in understanding the requirements for Design Science research. These guidelines have been used in section 3.2.4 to motivate why the Design Science research approach was applied in the study and used to illustrate how the study reached its intended goal and knowledge enhancement. The following part summarises the seven guidelines of Hevner et al. (2004).

Guideline 1: Design as an Artefact

METHODOLOGY

This first guideline specifies that Design Science must produce an artefact that is used in the Information Systems field. The artefact can also be the knowledge gained in the process of pursuing the research if the product is not entirely implemented. The artefact can also be a model or framework.

Guideline 2: Problem Relevance

This guideline states that the objective of a Design Science Researchers problem is to produce a solution that is pertinent to a particular problem.

Guideline 3: Design Evaluation

This guideline demands that the quality and the utility of the artefact must be evaluated through well-constructed methods.

The artefact needs to be evaluated according to specific criteria chosen beforehand by the researcher (Hevner & Chatterjee, 2010).

Guideline 4: Research Contributions

This guideline requires that Design Science research must produce a clear academic contribution to the area of investigation.

Guideline 5: Research Rigor

This guideline specifies that reliable Design Science research depends on the use of rigorous methods to construct and evaluate the artefact.

It is the way the research is conducted and is dependent on the environment in which the artefact will be applied or used. The rigour of research depends on the researcher's ability to select and apply appropriate methods and metrics used to develop and evaluate the artefact (Hevner, 2007). Methods and metrics should mostly come from the knowledge base of the area where the artefact will be applied. For research to be rigorous, the researcher must ensure that the artefact is thoroughly tested before the field release (Hevner, 2007). The researcher must also always ensure that the results are effectively coming from the data collected and the results respond to the research questions (Oates, 2006).

Guideline 6: Design as a Search Process

This part states that, for the artefact resulting from a Design Science research to be effective, it must have been developed through available resources to reach the desired aims.

Guideline 7: Communication of Research

This guideline advises that the resulting artefact must be shared with different audiences.

By following these guidelines, Hevner et al. (2004) aim to increase the value of Design Science in contributing to knowledge. Studies that are following these guidelines have a greater chance of contributing to the body of knowledge of their field.

3.2.4 Design Science Research Methodology

To facilitate the use of Design Science in practice, a Design Science Research Methodology has been developed by Vaishnavi & Kuechler (2007). Vaishnavi & Kuechler (2007) have divided the process into five steps: Awareness, Suggestion, Development, Evaluation and Conclusion. In the following section, these steps will be explained.

Figure 17 below demonstrates an overview of the Design Science Research Methodology.

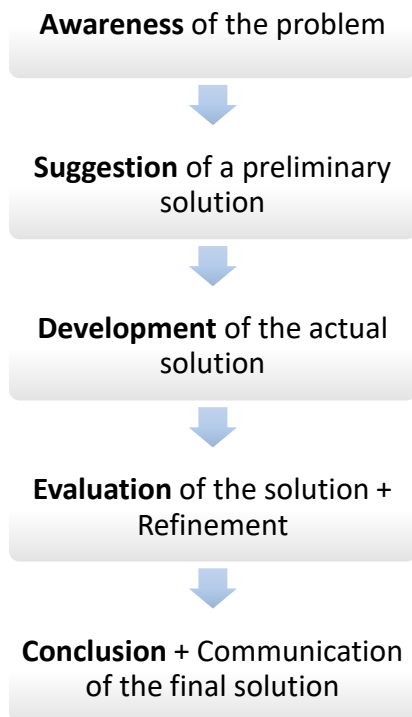


Figure 16 Overview of the Design Science Research Methodology steps (Vaishnavi and Kuechler, 2007)

Step 1: Awareness of the Problem

At this step, the researchers need to identify a potential problem that can be fixed. It can be done using several methods:

- Identifying a gap between the current state-of-art and an ideal state-of-art through the review of the literature
- Identifying the needs or problems of the intended users

The output of this step is a detailed explanation of the problem that will be addressed throughout the study in the form of a proposal for a new research effort. The statements made in the awareness phase will serve as guidelines to develop the solution in the development phase, as well as finding suitable and relevant evaluation criteria for the evaluation phase.

Step 2: Suggestion

Following the awareness of the problem, at this step, the objective of the solution must be identified. Suggestions come from examining the body of knowledge and the skills and level of understanding of the audience.

The result of this step is either a proposition of possible solutions or the possible components the final solution should have, as well as a provisional design.

Step 3: Development

At this step, one of the solutions proposed is investigated in detail. This solution is then designed, developed and implemented partially or fully, depending on the scale of the research. The output of this step is the actual artefact. Typical artefacts can be in the form of technology-based artefacts like frameworks, new systems or practices, organisation-based artefacts like structures and social systems or people-based artefacts like training.

Throughout the development phase, proper developmental strategies need to be applied to produce the artefact. Several popular development methodologies are successfully used, for example, waterfall and agile methodologies, as well as prototyping.

Prototyping is usually seen as an approach for handling a part of a development cycle, rather than a well-established development technology (Centers for Medicare & Medicaid Services (CMS), 2008). Prototyping is an iterative model where the users are directly involved in the cycle and increases the likelihood of user acceptance of the final product (ISTQB Exam Certification, n.d.).

The ISTQB Exam Certification (n.d.) website proposed an interesting model for prototyping which can be linked to the Design Science Research Methodology.

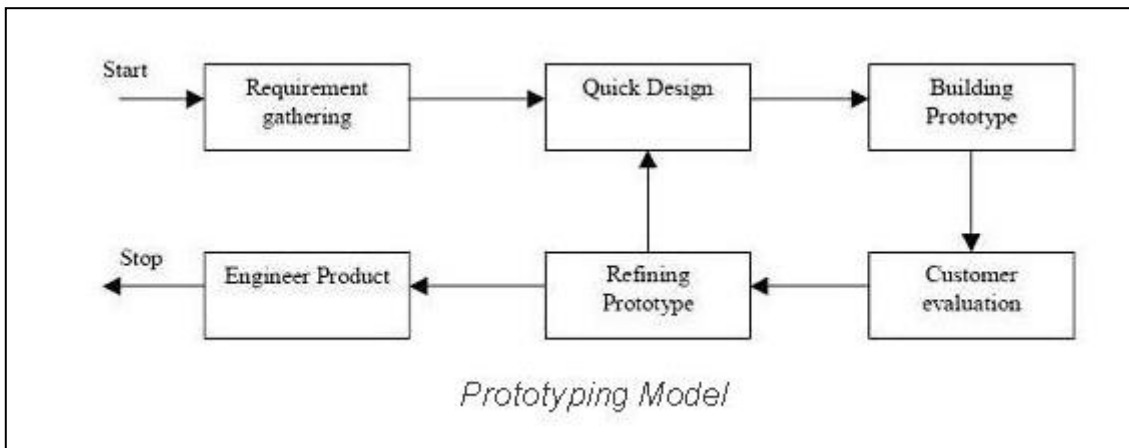


Figure 17 ISTQB Exam Certification - Prototyping Model (ISTQB Exam Certification, n.d.)

The choice of the most appropriate methodology will depend on the type of artefact developed (Vaishnavi & Kuechler, 2004). For example, Oates (2006) proposes the use of prototypes in the design research development phase. Prototypes are very common because they portray an early stage of the solution, and the users can test and refine them (Freetutes, n.d.).

The outcome of the development step is an actual artefact that can be used and tested.

Step 4: Evaluation

At this step, the actual artefact needs to be tested and evaluated by the intended user. The evaluation must provide the evidence that the artefact will solve the problem or provide useful updates and changes to make the solution more accurate. The feedback received after such an evaluation must be used to refine the artefact.

Hevner and Chatterjee (2010) stated that the evaluation step is done to ensure that the artefact meets the requirements and improves the current situation. It also contributes to the credibility and validity of the research.

Venable (2006) categorised Design Science Research evaluation into two forms: artificial and naturalistic evaluations. The evaluation in an artificial setting includes, but is not limited to, laboratory experiments, simulations, mathematical proofs or theoretical arguments (Pries-Heje, Baskerville and Venable, 2008). Artificial evaluation is therefore, somehow,

METHODOLOGY

unreal (simulation, hypothesis) and may not apply to real use. According to the three realities proposed by Sun and Kantor (2006), the artificial evaluation will be implemented to unreal users who will use a fictitious product to solve imaginary problems. Unlike artificial evaluation, naturalistic evaluation explores the performance of the artefact within its intended environment, for example at school or in an organisation. It consists of real users using a real product to solve a real problem, which these users have most likely encountered before (Sun & Kantor, 2006). It embraces the complexities of the human nature (Sun & Kantor, 2006), but might be expensive or difficult (Pries-Heje, et al., 2008) mostly because the interpreters could confound the recurrent variables or misinterpret the results. If it is done in the best possible way, the results of the naturalistic evaluation might be the most reliable for the real situation. The naturalistic evaluation includes, but is not limited to, field studies, case study, surveys, action research and hermeneutic methods (Pries-Heje, et al., 2008).

The evaluation criteria must be fair and followed by all people participating in the evaluation. Oates (2006) suggested that these criteria align with the research objectives. The criteria must come from the recommended essential elements of the proposed solution and the awareness phase.

Oates (2006) proposed the following evaluation criteria: functionality, completeness, consistency, accuracy, performance, reliability, usability, accessibility and aesthetics. Each evaluation criterion must be known and followed by the evaluators because each evaluator might want to assess the solution differently (Hevner & Chatterjee, 2010). It will assist in aligning the comments and ease the analysis.

The outcome of the evaluation can either be suggestions to modify the process used to get to the artefact, or the artefact itself (Oates, 2006). An iteration of the Design Science may be made up of the evaluation again, or changes can be implemented directly, and the process continues to the conclusion phase. Also, if no modifications are suggested after the assessment, the cycle will continue on to the next step.

Step 5: Conclusion

At this step, the research needs to be concluded, and the final artefact needs to be shared with the public. The input to the body of knowledge and the impact of the research, as well as future studies, need to be stated clearly.

Design Science studies need to be informed by existing theories and by operational requirements of the artefact (Hevner, et al., 2004).

The next section will discuss the way in which Design Science Research was implemented in this study

3.3 DESIGN SCIENCE RESEARCH METHODOLOGY APPLICATION

Figure 18 below shows the Design Science Research Methodology's steps, as implemented in this research. The research was done in different design cycles. The main cycle's focus was the design of the central artefact, namely the framework. Two artefacts, which contribute towards the final framework, were developed in two separate sub-cycles. The two artefacts are the Cyber Safety Information Needs Assessment Instrument (which can be used to determine the cyber safety information needs of parents), as well as a preliminary categorisation of available cyber safety material suitable for parents. Figure 18 below outlines the main cycle and how the two sub-cycles fit into the development of the final framework.

METHODOLOGY

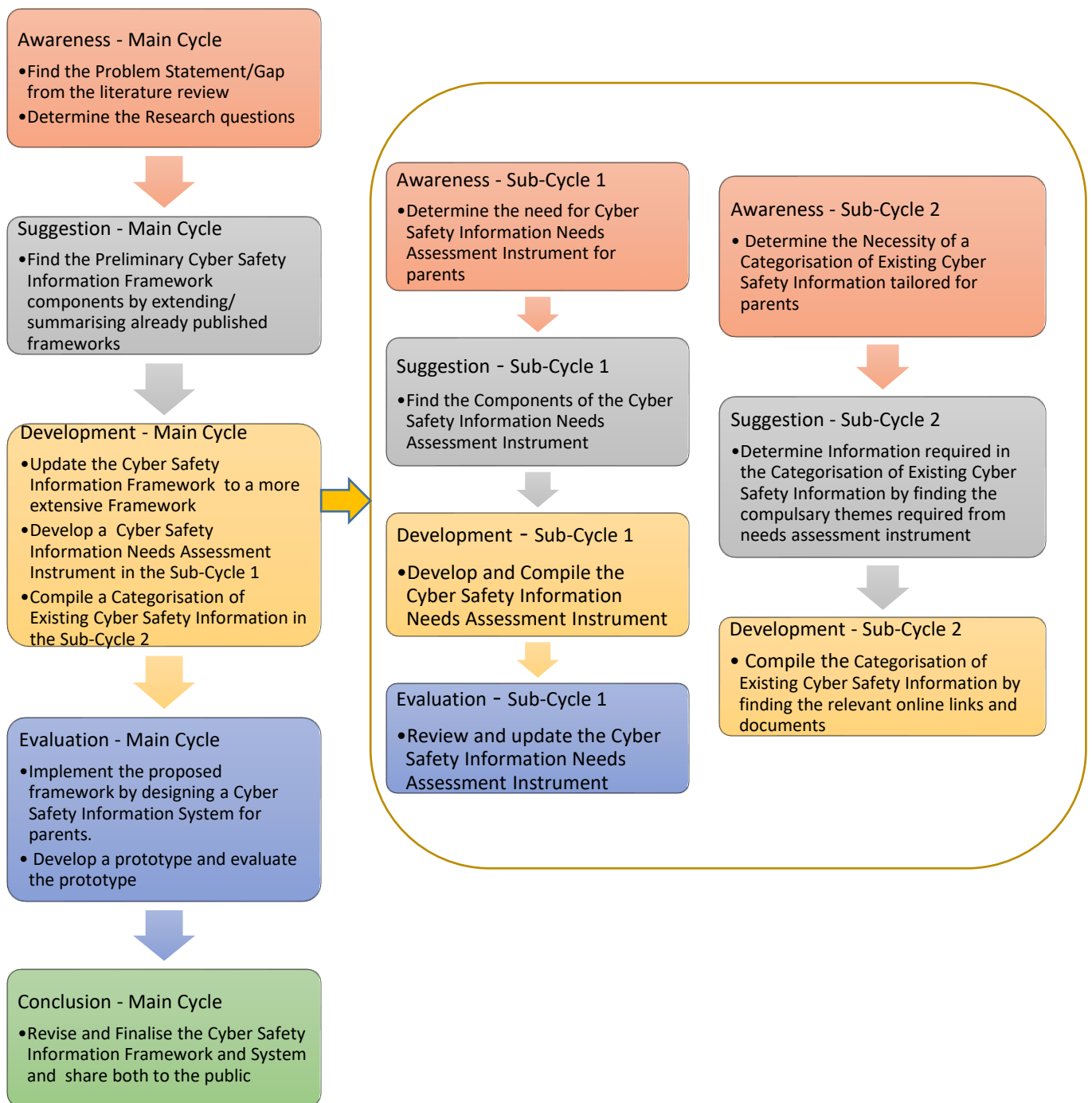


Figure 18 Design Science Research Methodology Application (adopted from (Vaishnavi and Kuechler, 2007))

Each of the development cycles will be discussed below.

3.3.1 Main Cycle

Figure 19 below gives an overview of the outcomes of each step of the main cycle.

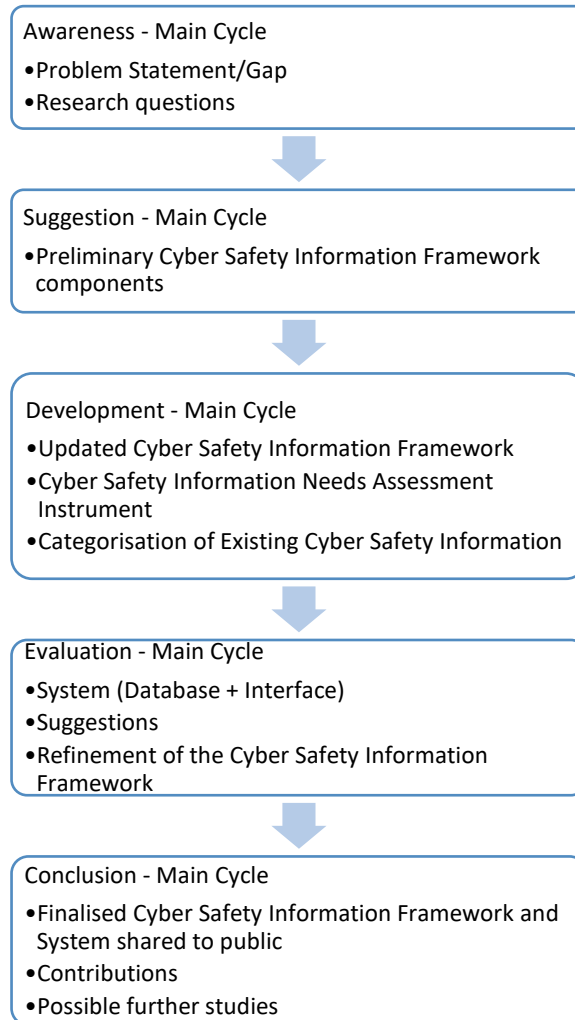


Figure 19 Overview of the Outcomes of Each Step of the Dissertation's Design Science Research Methodology (Vaishnavi and Kuechler, 2007)

3.3.1.1 Step 1: Awareness of the Problem

Through the literature review, the issue of the lack of knowledge of the cyber safety of parents has been exposed. The awareness of the problem was done thoroughly in chapter 2 and will be summarised in Section 4.1.

The literature review in chapter 2 indicated that parents and teachers are not familiar with, and feel overwhelmed by new technologies (Hollingworth, et al., 2009). Parents and teachers are, therefore, ill-prepared for the cyber safety education and awareness of their children (de Lange & von Solms, 2012). Parents need efficient but straightforward material that will teach them what one needs to know about the internet and communication technologies to allow them to educate their children in this regard. In addition, an informal discussion held with Edu X (the service provider) added to the awareness of parents' issue. Edu X (pseudonym) is a privately-owned service provider in South Africa who provides a platform and support to schools who would like to implement the use of internet and digital devices to their curricula. More information about the context of the research and Edu X will be given in section 3.3. Edu X mentioned a need for an application based on a Cyber Safety Information Framework that could be provided to their client schools to raise cyber safety awareness. In addition, as far as the researchers know, there are no cyber safety information frameworks targeted for parents (von Solms & von Solms, 2015).

3.3.1.2 Step 2: Suggestion

Existing frameworks from (de Lange & von Solms, 2012) and (Dlamini, et al., 2011) were used to come up with preliminary components of the framework, as well as how these components can be related. The Cyber Safety Information Framework is based on three main elements and will be discussed in more detail in section 4.2.1:

- A set of components of a Cyber Safety Information Framework (based on de Lange and von Solms, 2012 and Dlamini, et al., 2011)
- A parents' Cyber Safety Information Needs Assessment Instrument (CSINAI). Through this, parents' initial awareness of cyber safety, their digital literacy, the age of their children and their information and information dissemination needs can be determined.
- The categorisation of existing cyber safety Information: A categorisation of cyber safety topic(s) for which there exists a need.

These components were inspired by the requirements gathered in the literature review and adapted to the cyber safety awareness and parental context, and are discussed in more detail in chapter 4, section 4.2.1.

3.3.1.3 Step 3: Development

At this step, the actual solution needs to be designed. Supported by the answers acquired from the parents, and a checklist for the kind of information cyber safety awareness material should contain, the framework components were adjusted.

A first design sub-cycle was entered into to develop an instrument with which to determine the needs of parents before starting an awareness campaign. Data has been collected through questionnaires given to the participants during a parents' meeting at school to portray the actual need for a cyber safety awareness campaign for parents. Also, published material such as academic articles, reports, online resources on cyber safety and other related topics have been gathered and analysed to find existing frameworks and theories to document in the questionnaire.

This questionnaire was tested at School X using Edu X's solution. The findings were used to refine the instrument and inform the next sub-cycle.

In the second sub-cycle, existing cyber safety material available on the internet was indexed according to parent's needs (depending on their awareness, digital literacy, children's age and cyber safety information needs).

The final step of the development involved the refinement and presentation of the updated framework, to be evaluated by intended users.

3.3.1.4 Step 4: Evaluation

At this step, the actual artefact needs to be tested and assessed by the intended user, and then changes must be made accordingly. To evaluate the Cyber Safety Information Framework, it has been instantiated by designing a small system which can be used by the

service provider, Edu X. The design only entails the database and a Cyber Safety Awareness Form design. This instantiation was then shared with the service provider to validate its relevance. The instantiation also came with evaluation criteria. Since this was only a design of a system, and not a working system, the researchers focused on the evaluation criteria as functionality (usefulness to their needs), usability (the ease to use), completeness, aesthetics and their expectation vs what the researchers have provided them, inspired by the criteria proposed by Oates (2006). The researcher received feedback about the framework and its instantiation from a representative of Edu X during an interview session. According to the input received, the instantiation and the framework were updated.

3.3.1.5 Step 5: Conclusion

At this step, the final artefact needs to be shared with the intended user. The Cyber Safety Information Framework, as well as its instantiation, were shared with the service provider and updated according to their feedback. In addition, a first version of the framework was published in the conference proceedings of the 2016 African Cyber Citizenship Conference (Paraiso & Matthee, 2016).

At this step, contribution to the BOK needs to be established, as well as possible future research.

This Design Science research approach was appropriate, since the outcome of this study was a framework which could be seen as an artefact. Design Science research artefacts can comprise models, methods, constructs, design theories, frameworks and instantiations (March & Smith, 1995). The framework resulting from the study can be used to create a Cyber Safety Information application, which can be used by schools to educate parents. The resulting application will help to bridge the gap between what parents currently know about Cyber Safety, and what they are supposed to know.

Hevner (2007) proposed three cycles that needed to be taken into consideration to help apply Design Science research in IS in the most efficient manner. The Relevance Cycle bridges the contextual environment where the research is taking place with the activities

METHODOLOGY

performed in Design Science. The Rigor Cycle connects the Knowledge Base of expertise, foundations and experience acquired on different studies. The Design Cycle focuses on the activities to design and evaluate the artefact created using Design Science research.

Inspired by the figure proposed by Hevner (2007), the following illustration (Figure 20) will show how the research was conducted using these three cycles. It will also depict how the researchers ensured that Design Science research was performed efficiently and ensured the artefact created filled the gap identified in the introduction of the research.

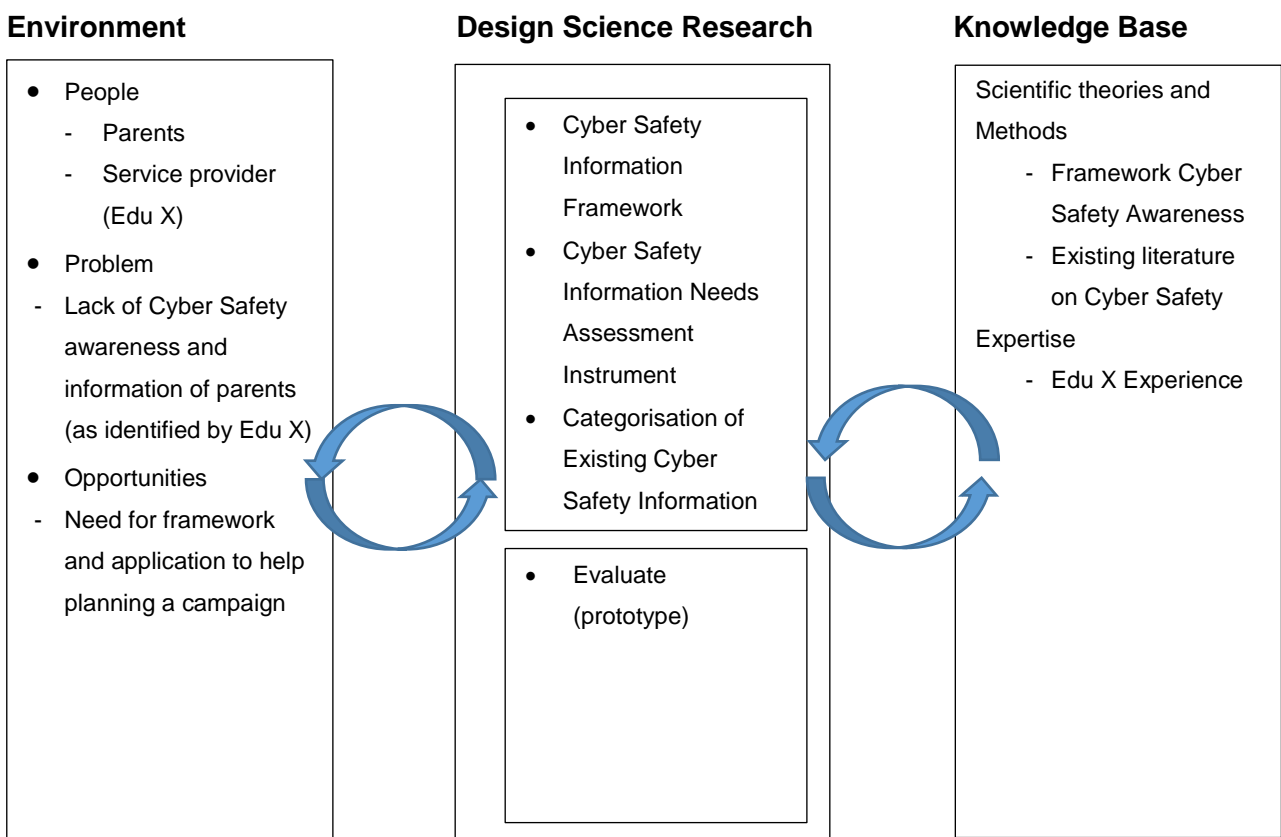


Figure 20 Adaptation of Design Science Research Cycles According to Our Research (Hevner, 2007)

3.3.2 Sub-Cycle 1 – A Cyber Safety Information Needs Assessment Instrument (CSINAI) for Parents

Figure 21 below gives an overview of the outcomes of each step of the Sub-Cycle 1.

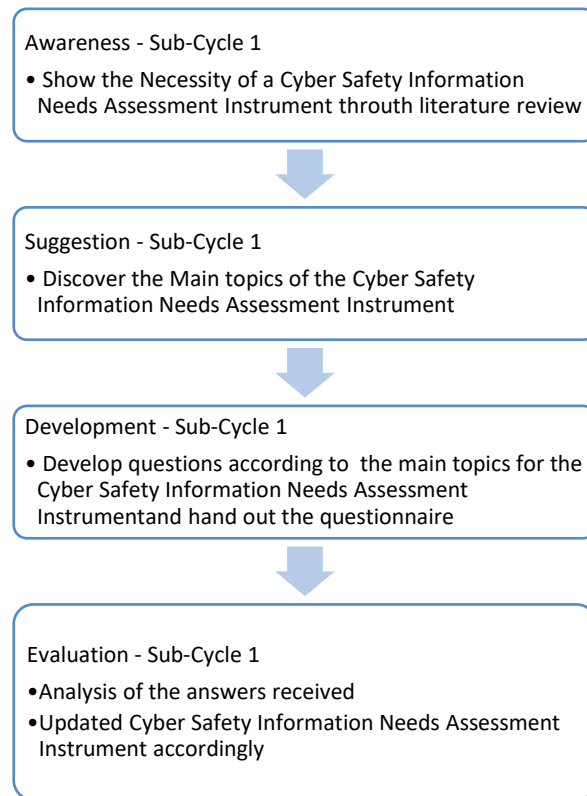


Figure 21 The Different Design Science Research Methodology Phases of Sub-Cycle 1

3.3.2.1 Awareness

The literature review in chapter 2 of the study has helped to emphasise the necessity of an instrument that will help assess the needs of the intended audience before a cyber safety awareness campaign can take place. The literature review has developed that for a campaign to be useful, the needs of the audience need to be discovered beforehand. Their needs mainly comprise their initial knowledge of the topic (Cyber Safety), their preference in the way they would like to receive the training, the relevant topics and the age of their children. Because the researchers were dealing with cyber safety (which implies computers, mobile devices and the internet), the literature review has also emphasised that the level of knowledge of these tools also required an assessment. An informal discussion held with Edu X highlighted that they need an application where one can collect information about the

intended audience at the client school to provide them with tailored awareness information, along with their services.

De Lange and von Solms (2012) as well as Dlamini, et al. (2011), have highlighted that one should identify the needs of the audience in order to create a relevant campaign.

3.3.2.2 Suggestion

The CSINAI was inspired by the five components of the original framework of De Lange and von Solms (2012). This framework has assisted in identifying three main subjects that needed to be covered in the instrument, namely the digital literacy, the cyber safety and the communication preferences of parents.

The digital literacy section will help highlight the parents technological and internet abilities, and the Cyber Safety Section will help determine their knowledge of the common cyber safety terms and jargon. Communication preferences will help define their availability and preferred delivery method, as well as if parents are aware of schools and government cyber safety policies (if applicable).

Using the CSINAI will assess the parents (WHO factor) original *Digital Literacy* and *Cyber Safety* levels to determine the depth of the information provided during the training and avoid redundancy. De Lange and von Solms (2012) refer to the WHAT and the WHERE factors and their *Communication Preferences* to refer to the WHEN, HOW and GOVERNANCE factors.

3.3.2.3 Development

The Cyber Safety Information Needs Assessment Instrument has been developed in this phase. It was done according to the components of the preliminary framework, as well as determining cyber safety themes from the literature. The questionnaire, which served as an initial version of the CSINAI, centred around three themes: digital literacy, cyber safety awareness and presentation type. Each part comprised questions that assisted in detailing

the topics. The kind of questions used in each section has been decided on through the analysis of the review of the literature.

In the sections below, the research approach followed in this Sub-Cycle is explained in more detail.

3.3.2.4 Evaluation

The evaluation of the CSINAI has been done by letting parents complete the questionnaire and conducting follow-up interviews. The analysis of the data collected has been used to compile the final version of the CSINAI for parents. Table 2 and Figure 22 below summarise the different steps of this Sub-Cycle, with its data collection and analysis method.

Table 2 Summary of Data Collection and Analysis Approaches in Sub-Cycle 1

Design cycle phase	Data collection	Data analysis	Deliverable
Awareness	Literature study		N/A
Suggestion	Literature study	Thematic analysis	N/A
Development			The first draft of the Cyber Safety Information Needs Assessment Instrument
Evaluation	Questionnaire and interviews	Descriptive statistics and thematic analysis	Cyber Safety Information Needs Assessment Instrument

3.3.2.5 Research Methodology Followed in Sub-Cycle 1

The research design of this phase was a case study. Case study research chooses a limited number of people, or a specific area and condition, as their sample or subjects to study in order to view a situation within a particular context (Zainal, 2007). It allows exploring real-life phenomenon through a detailed analysis of events and their connection (Zainal, 2007).

The school (School X) where the study took place, is a member of the privately-owned group of schools, Care (pseudonym), situated near Pretoria. Their mission is to make independent

schools accessible to learners. Care has several brands in the group, which accommodate learners from 3 months to Grade 12. After a pilot study in 2012, the group implemented technology in their educational processes from 2013. Care is using the e-textbook platform of Edu X and provide tablets and electronic study material to learners. School X is a new addition to the schools of Care and was opened in 2014. It has implemented the use of technology in their school from 2016. The implementation is done in phases and only selected grades are currently using the technology. Similar to the other Care schools, Edu X uses the platform provided by Edu X. Since this is a recent implementation and since the parents come from various socioeconomic strata, this school seemed ideal for this research.

At registration, learners from certain grades (8 and 10) receive an Android-based tablet with e-books and access to the Edu X platform where additional material like homework, past exam papers, informative videos and other interactive content, can be downloaded. Their teachers can push content into their textbooks beforehand. Teachers have access to a more advanced view where they can set up the content to be accessed by their class. Learners without internet at home can download the extra resources at school. The learners take these tablets home to do homework and study for tests and exams. The e-textbooks are also only available on the tablets. The e-books received can be used exactly as the printed books are. Content can be highlighted, and learners are able to make a note in them if they wish to. Learners can also have access to interactive content (like animations) to enhance their interest in learning.

Edu X is based in Pretoria, and has support personnel at the school a few days per week. Edu X is a South African ICT education company who provides an e-textbook platform as part of a suite of e-learning offerings. Their solution is implemented in both private and public schools in all of the nine provinces. The proposed Cyber Safety Information Framework (as the outcome of this research) can be used by Edu X to enhance their services.

3.3.2.5.1 Data Collection

There are several ways of collecting data, and this research has used various methods. In this cycle, the research has used the suggested Cyber Safety Information Needs

METHODOLOGY

Assessment Instrument as questionnaires to obtain qualitative and quantitative data to refine and evaluate the Cyber Safety Information Needs Assessment Instrument.

Some of the data collection methods that are used in qualitative research are interviews, observation, questionnaires, surveys, gathering information from archives and literature and focus groups (Myers, 2013). The researcher used unstructured interviews with the parents of School X after they completed the questionnaires. These findings were also used to inform the refinement of the Needs Assessment Instrument. It brought to the attention of the researcher that certain questions were obsolete, where others had to be added.

Because the researchers did not want the study to be limited to only people with internet access and digital devices, the questionnaires were printed and shared with the respondents during a parents' meeting at the school. More details are given in the following section. The questionnaire questions were carefully chosen to avoid misunderstanding. The questionnaires comprise open-ended and closed questions (see Appendix A) and were divided into three sections. The first section was about digital literacy, which tried to establish the level of comfort each respondent has with technology and the frequency of which he or she uses it. The second section was about the respondents' awareness of cyber safety, and assisted in evaluating their knowledge of cyber safety threats and determining how severe and critical the respondents see each one of them. The third section covered presentation type and responsibilities. This section tried to discover what would be the preferred type of presentation material during a campaign, as well as whom they think must be responsible for the cyber safety awareness training of the community.

The answers to the questionnaire were anonymous, and no personal information was collected. The responses to the questionnaire have helped find communication preferences and key topics for the parents of the school. More is said about the findings in section 5.4.

3.3.2.5.2 Sampling Method

The study has used purposive sampling. Purposive sampling involves the use of individuals in a group of people who have a particular knowledge or experience of a certain phenomenon or situation (Cresswell & Plano, 2011). For purposive sampling, it is also

METHODOLOGY

paramount that the participants be willing and available to participate in the study (Bernard, 2002), as it will help get a better picture of the situation.

Data was collected during a high school parents' meeting evening. Twice a year, the principal, teachers and parents have a meeting to discuss the issues encountered at the school with the children in general and find a way forward together. When parents arrived, they were given the agenda of the meeting along with the questionnaire and some explanation about the purpose of the research. Near the end of the session, a friendly reminder was given to the parents to not forget about the questionnaire. The questionnaire was returned at the end of the meeting.

3.3.2.5.3 Sample Size

The high school has 209 learners registered this year (2016). The researcher anticipated the same number of parents present at the meeting. Unfortunately, roughly half of them attended the meeting and 55 parents responded to the questionnaire.

The research has only considered 48 questionnaires because the other seven were not entirely complete or some of the pages were missing.

3.3.2.5.4 Data Analysis

Data analysis is a critical part of the research. It includes examining, transforming and moulding data aiming to learn new insights and suggest deductions from information collected (Statistics Canada, 2009).

Analysing data obtained from mixed methods consists of interpreting qualitative data using qualitative methods and quantitative data using quantitative methods (Creswell & Plano Clark, 2007). The analysis of both types of data can be done simultaneously or the analyses of either the quantitative or qualitative data can be done first and will inform and influence the results of the other (Onwuegbuzie & Teddlie, 2007).

The next sections will demonstrate how data has been analysed in detail.

3.3.2.5.4.1 Qualitative Data Analysis

Qualitative data requires analysis and interpretation of the data gathered (Alhojailan, 2012). For the analysis of qualitative data, Denscombe (2010) cited a few principles, which if followed, will maximise the efficiency of the research's results. The first principle is that raw data needs to be compacted into concise information in tables or charts. The second principle is to clearly form relationships between the research objectives and the concise information. The third principle proposes that the research should be concluded by developing a model and/or improving the abstract root of the research.

In this context, thematic analysis was used to decipher the data gathered. Generally, thematic analysis is used in qualitative data (Jugder, 2016). Braun and Clarke's (2006) views predominately influence the way thematic analysis is understood in this research. According to them, thematic analysis is a method in qualitative research to analyse and report recurring patterns and themes in the collected data. Braun and Clarke's considered a theme as being a key idea from the data collected in correlation with the research question. This key idea should create some pattern responses in the data (Braun & Clarke, 2006). Themes can be identified using an inductive or deductive strategy, depending on the data set. Moreover, a rigorous thematic analysis can produce intuitive and profound answers to research questions, and one of its greater advantages is its simplicity and versatility. It can be adapted to several types of research according to their outcome (Braun & Clarke, 2006) and aids illustrating data in relevant detail also assesses several subjects by interpretation (Boyatzis, 1998).

Qualitative data was collected from the open-ended questions of the questionnaire, as well as the unstructured interviews conducted afterwards. The answers to each question have been transcribed, and themes and patterns have been drawn from them. More detailed information on how the analysis took place, and which themes were identified, is given in chapter 5.

3.3.2.5.4.2 Quantitative Data Analysis

Only descriptive statistics were used to analyse the responses to the closed questions. The focus was mainly on the frequency distribution of the answers to determine the most prevalent needs of the parent.

3.3.3 Sub-Cycle 2 – A Categorisation of Existing Cyber Safety Information for Parents

Figure 22 below gives an overview of the outcomes of each step of the Sub-Cycle 2.

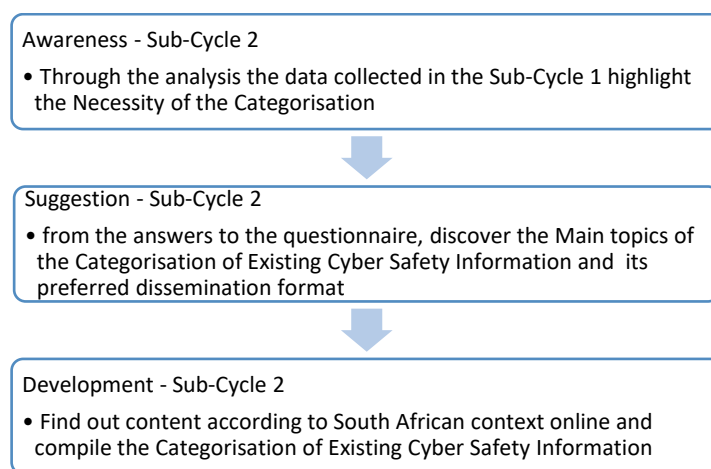


Figure 22 The Different Design Science Research Methodology Phases of Sub-Cycle 2

3.3.3.1 Awareness

From the data collected through the questionnaire (instrument) and the interviews, the topics parents of the school would like to have more information about, were identified. This analysis has also shown in which format parents would like to receive the information. It is now imperative to know which information, which is already available, can be used in any cyber safety awareness campaign. The necessity of a categorisation of existing online cyber safety information has been emphasised during Sub-Cycle1.

3.3.3.2 Suggestion

Since there exists ample online material on cyber safety for not only children, but also adults, the idea was to categorise existing material according to themes and ages of children, similar to the work done by von Solms and von Solms (2014): having a starting point and then enhancing it with results from the questionnaire. The parents identified some topics through the questionnaires.

3.3.3.3 Development

The South African online content was mainly categorised according to themes, topics, sub-topics, HTML links, age group and presentation type. The data included in the categorisation was taken from published documents and online resources. The categorisation is in the form of a report with topics and related links to relevant information.

3.3.3.4 Research Methodology Followed in Sub-Cycle 2

To compile a complete and relevant categorisation, a literature review was done. Previous categorisation and studies were consulted in order to have an idea of what has already been done and what the researchers should improve on.

Results from Sub-Cycle 1 were also used as an indication of the type of document the categorisation should be.

3.3.3.4.1 Data Collection

To compile their required categorisation, online searches were used in Sub-Cycle 2 as a data collection method. Using online studies as data collection methods has arisen out of the increased use of the internet (Mukherjee, 2012), and it gives access to unlimited sources of information. Before selecting data, which will be part of the research, information will need to be certified and come from trusted sources. Data taken online has the advantage of being dynamic as the quality of the information coming from a given source can be improved, but it can also be a drawback as links can be removed and the sources can become obsolete (Mukherjee, 2012). More detail about the method used is given in chapter 6.1.3.

3.3.3.4.2 Data Analysis

The online content was analysed by categorising it, and topics, themes and sub-themes were determined. However, judgment regarding age group was sometimes subjective. Also, the researcher used her own opinion regarding the presentation type. Themes and sub-themes have allowed choosing the type information comprised in the categorisation.

Table 3 Summary of Data Collection and Analysis Approaches in Sub-Cycle 2

Design cycle phase	Data collection	Data analysis	Deliverable
Awareness	Sub - Cycle 1 and literature study		
Suggestion	Results from the literature study and existing Cyber Safety Information Needs Assessment Instrument		
Development	Document	Use existing dimensions to do the categorisation	The categorisation of online content

Table 3 above gives a summary of the methodology used for the Sub-Cycle 2.

3.3.4 Summary of Research Approach

Table 4 provides an overview of the data collection, data analysis and artefact created in each cycle, including the main cycle.

Table 4 Summary of the Research Approach

Research question	Design cycle	Data collection	Data analysis	Deliverable
1. What are the cyber safety threats of using mobile devices, especially for learning purposes?	Main cycle (awareness)	Literature study		

METHODOLOGY

<p>2. What is being done locally and internationally to make parents aware of cyber safety in schools and at home?</p>	<p>Main cycle (awareness)</p>	<p>Literature study</p>		
<p>3. What measures are being taken by schools in South Africa to inform parents about the cyber safety-related issues when they are implementing the use of mobile devices?</p>	<p>Main cycle (awareness)</p>	<p>Literature study</p>		
<p>4. How can the information's needs of parents be determined in the South African context regarding cyber safety awareness?</p>	<p>Sub-Cycle 1</p>	<p>Literature study, Questionnaire</p>	<p>Descriptive statistics and thematic analysis</p>	<p>Cyber Safety information needs assessment instrument for parents</p>
<p>5. How can existing cyber safety information be categorised to fulfil South African parents' needs?</p>	<p>Sub-Cycle 2</p>	<p>Documents</p>	<p>Categorisation using existing dimensions</p>	<p>The categorisation of existing Cyber Safety material</p>
<p>6. What would an instantiation of the framework look like?</p>	<p>Main cycle (evaluation)</p>	<p>Interview</p>	<p>Thematic analysis</p>	<p>Design of an instantiation of the framework Refined Cyber Safety Information Framework for parents</p>

3.4 ETHICAL CONSIDERATIONS

The most common way of defining ethics would be a set of regulations that became norms. These regulations specify what is considered as right or wrong within a population, and might be learned at home, school, media or from the present society (Resnik, 2011).

It is imperative to submit to global norms of ethics in research because it encourages the principal purpose of doing research. It helps to gain a broad understanding of the subject knowledge, being honest and avoiding inaccuracies in the results. Norms also help others understand better in order to get the best out of their answers. It is a core requirement for qualitative research which works around people's perceptions of the world. Furthermore, ethics help the researcher to gain trust, which may attract more sponsors for the research if needed. Finally, norms contribute to making sure the researcher complies with social responsibilities and is in accordance with the law, human rights and animal welfare (Resnik, 2011). Not complying with these rules and norms in research might harm the researcher or the participants or prevent the research from being sponsored or reliable.

After the questionnaire's questions were established and approved by the school where the research took place, an ethical clearance was obtained from the University of Pretoria EBIT Ethics Committee.

The research will not expose respondents as their identity or precise information will not be kept on record.

Participants will never be asked to partake in illegal or universally unethical actions, and will always have the choice to leave and be removed from the study.

The resulting Cyber Safety Information Framework materialised as a design of a system and was presented to the service provider to be evaluated and refined to make sure their requirements, as well as the parents' needs, have been addressed.

3.5 CONCLUSION

Chapter 3 discussed the Design Science research methodology that was used for the study to achieve the research objectives. The next chapter gives the awareness and suggestion phase of the main cycle.

4 AWARENESS AND SUGGESTION – MAIN CYCLE

4.1 AWARENESS – NEED FOR A CYBER SAFETY INFORMATION FRAMEWORK FOR PARENTS

This awareness phase defines the current state of cyber safety awareness among parents and their children, assisted by considering current literature. The awareness phase will also portray the ideal state of cyber safety awareness to identify where the gaps, which need to be filled, lie.

4.1.1 Awareness Overview

In South Africa, to respond to a need for a “tech-savvy” population, various actions have been taken to implement the use of technology in schools. These initiatives would imply that learners might be educated on the issues of their safety and security when using technology and the internet. Thus, learners need to be guided on how to adopt safe online behaviour. This education should preferably come from their home environments and be continued at school and with their peers. Unfortunately, parents are often less knowledgeable about technology than their children (Computer Science and Telecommunications Board - National Research Council, 2002) and often feel overwhelmed by their new learning and social environments (Hollingworth, et al., 2009).

Although some organisations are actively encouraging cyber safety education and awareness, there is a lack of well-structured guidelines for schools, teachers and parents to help them in reacting to, or avoiding, cyber-safety threats effectively (Sonhera, et al., 2012). Currently, no comprehensive cyber safety initiatives are in place, and schools lack relevant curricula (von Solms & von Solms, 2014). Most parents are not familiar with what is going on online or how they can support their children (de Lange & von Solms, 2012). Hence, there is a necessity for producing material that will provide tailored information on cyber safety for parents. During an informal discussion with a service provider, (Edu X) emphasised the need for materials to help them get to know their audience better and to provide them with the most appropriate resources for cyber safety awareness.

Providing customised information to parents will prepare them for the advancements so that they will be able to assist their children, as well as expand their own digital literacy level (Telstra Corporation Limited, 2014). Digital literacy refers to the skill set necessary to participate in the digital era. These skills include the ability to use technology, get the most out of its opportunities and tackle the challenges associated with it (Gilster, 1997).

4.1.2 Awareness Campaign Overview

The following components were the recurring parameters in the literature that need to be considered while organising an awareness campaign in order to compile accurate material for the intended audience.

Table 5 Component of Cyber Safety Awareness Campaign

Step	Component	Subcomponent	Source
1	Identify the Role-players		(de Lange & von Solms, 2012)
2	Choose the targeted audience		(Dlamini, et al., 2011)
3	Consult the overall Body Of Knowledge (internationally & in context) to find out	Trending topics Overall Cyber Safety requirements (digital literacy, personal skills, preliminary awareness) Available policies/rules/ laws Possible medium Possible support/ reaction procedure (recognition, mitigation, reaction, responsibility skills) Usual evaluation procedure	(Kritzinger & von Solms, 2012) (Dlamini, et al., 2011)
4	Identify the audience’s current skills		(Dlamini, et al., 2011)
5	Compare the audience’s skills against overall	Skills needed Topics needed to be covered	(de Lange & von Solms, 2012)

	requirements to isolate their specific needs	Preferred medium, time	(Kritzinger & von Solms, 2012)
6	Compile Material according to previous steps		(Dlamini, et al., 2011)
7	Arrange an actual training session	Venue Tips to keep audience interest during training Trainer and trainee availability	(Dlamini, et al., 2011)
8	Evaluate the impact of the training or the material		(Dlamini, et al., 2011)

The Awareness step above has shown (using the review of the literature) the need for basic materials that will be used by parents to educate themselves about cyber safety awareness, increase their digital literacy and create a safer cyberspace.

The following section will suggest a Cyber Safety Information Framework according to parents' requirements drawn from the awareness section.

4.2 SUGGESTION

The Suggestion phase of a Design Science research will help define a preliminary solution to bridge the gap discovered during the awareness phase.

4.2.1 Preliminary Cyber Safety Information Framework

The preliminary Cyber Safety Information Framework can be seen as an extension of the frameworks explained in the literature review (see section 2.6). The Cyber Safety Information Framework focuses on one of the Role Players, namely the *parents*, and on what is needed to compile accurate cyber safety awareness material for them.

For the purpose of this research, parents are seen here as *learners* who need to receive adequate training to become *teachers*, *identifiers* and *advisors*, as indicated by de Lange and von Solms (2012). It is assumed that the school already has policies and rules in place, so the aim of the Cyber Safety Information Framework would be to ensure that the parents are aware of them.

The figure below is inspired by the framework from the high-level e-Safety framework proposed by de Lange and von Solms (2012) and the review of the published literature. The researchers have proposed an adapted version which forms part of our suggested Cyber Safety Information Framework.

Table 6 Framework Components (Adapted from de Lange and von Solms (2012))

E-safety framework components	Adapted components
The CONTROL Factor	Governance
The WHO Factor	Parents
The WHAT Factor	E-Safety Topics
The WHERE Factor	Resources
The WHEN and HOW Factor	Delivery

The table below shows how the researcher used the Cyber Safety framework’s components of de Lange and von Solms (2012) to identify the parents current skills and what would need to be included in the material to be shared with them. The preliminary Cyber Safety Information Framework suggested here is, thus, an application of the e-Safety framework provided by de Lange and von Solms (2012) to a specific participant, namely, the parents.

Table 7 Extension Criteria for the Targeted Audience Only (Parents)

E-Safety Framework Components	Our Extension Criteria
Governance: The CONTROL Factor	What has been done/ given to parents by the school? Do parents clearly know what role they need to play?
Parents: The WHO Factor	What are the parents' needs in order to become effective teachers, advisors, and identifiers? What are their existing cyber safety awareness levels? What are the parents' current digital literacy skills? What is the age of their children?
E-Safety Topics: The WHAT Factor	Which topics do parents indicate as essential to be made aware of? Which topics should parents be aware of?
Resources: The WHERE Factor	According to their needs, how should the information be conveyed? Where can one find such information?
Delivery: The WHEN and HOW Factor	When should the awareness campaign take place? How should the information be conveyed?

From the above table, it is clear that school governance influences all other components. The policies provided by the school should inform parental roles, important e-safety topics and the way in which information sessions/interventions will be conducted. On the other hand, parents should be able to communicate with principals or teachers about their cyber safety concerns and their needs which will again influence policies. It also shows that the chosen topics will determine the resources and delivery thereof, but that parents have specific requirements regarding the information sessions' format. Figure 23 below shows the relationship between the different components.

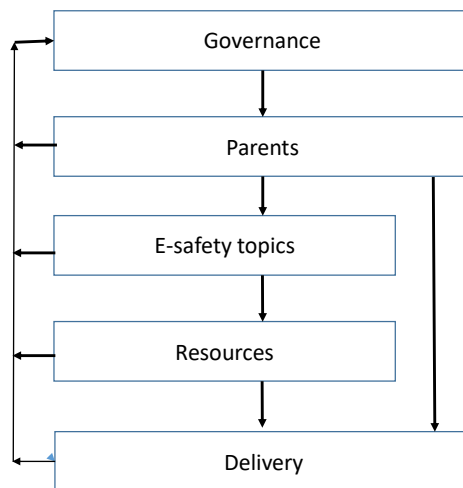


Figure 23 Preliminary Cyber Safety Information Framework

4.3 CONCLUSION

This chapter depicts the two first steps of the Design Science Research Methodology of the main cycle of the research, namely, the awareness and suggestion phases.

In the awareness phase of the main cycle, using the literature review done in the second chapter of the study, the researchers showed the current state of cyber safety awareness globally and in South Africa, and the ideal state of awareness. It was used to find where the gap between the two lies.

Knowing where the gap lies, the researchers suggested a solution in the suggestion phase, which is a Cyber Safety Information Framework to assist in raising the awareness of the parents. This preliminary framework was fundamentally from previously published frameworks.

AWARENESS AND SUGGESTION – Main Cycle

The following chapter describes the two sub-cycles of the main cycle where two instruments/tools are suggested and developed to enhance the preliminary Cyber Safety Information Framework.

5 DEVELOPMENT – SUB-CYCLE 1: CYBER SAFETY INFORMATION NEEDS ASSESSMENT INSTRUMENT

The development phase of Design Science research will help construct the actual solution to the gaps discovered in the previous phases. This sub-cycle focuses on the development of a Cyber Safety Information Needs Assessment Instrument (CSINAI) for parents.

5.1 AWARENESS

According to the second to fourth steps of the awareness campaign overview (Table 5) and the preliminary Cyber Safety Information Framework (**Error! Reference source not found.**), the needs of the parents must be established before the campaign takes place. The needs of the parents will determine the way in which the components of the proposed framework will be put together. The preliminary framework suggested in section 4.2.1 can, therefore, be enhanced by providing an instrument that can be used to determine the cyber safety information needs of parents. This instrument will help to provide tailored information to the intended audience.

5.2 SUGGESTION

The suggestion is that most of the components of the preliminary Cyber Safety Information Framework be used to develop the CSINAI.

Governance: Parents should be asked whether they are aware of the school's policy regarding cyber safety.

Parents: Their digital literacy and current cyber safety awareness should be assessed.

Cyber Safety topics: The choice of topics to be included in the assessment instrument should be based on existing research. Also, parents need to indicate which topics they need information on.

Delivery methods: Parents should be asked how they prefer to be informed about cyber safety issues.

Delivery time: Parents should be asked when the preferred time or event would be to receive awareness on safety issues.

The instrument, therefore, needs to be able to specify the current cyber safety awareness of the intended audience, namely the parents, their digital literacy and their ideal method and time of delivery.

5.3 DEVELOPMENT

The CSINAI has been developed along the lines provided in the suggestion phase. It is a questionnaire divided into three sections discussed in more detail below:

Section 1: The first section comprises nine questions testing the level of digital literacy of the respondents. The topics related to the evaluation of digital literacy were obtained from the frameworks proposed by Dlamini, et al. (2011) and von Solms & von Solms (2014). This section is meant to shed more light on the **Topics** and **Parents** component of our proposed Cyber Safety Information Framework. Parents were also asked about their usage and general knowledge of technology. It will assist in defining the starting point of the training, as well as the depth of the information provided during the session.

Section 2: The second section consists of eleven questions testing parents' current knowledge of cyber safety awareness. Parents were asked about their understanding of specific safety issues chosen according to Kritzinger's (2015) categories discussed in chapter 2. This section forms part of the themes identified in the literature review, as well from the research from von Solms & von Solms (2014) , this section will also bring more details about the **Topics** and the depths of the information provided during the training.

Section 3: The third section comprises thirteen questions to determine their delivery preferences according to the **Delivery** methods and time requirements in the framework proposed by de Lange and von Solms (2012).

In this section, parents were also asked about their awareness regarding the school's cyber safety policy, in accordance with the **Governance** requirements of the framework proposed by de Lange and von Solms (2012) and used in our Cyber Safety Information Framework.

The questions are short and concise to avoid misunderstanding of the topics and to achieve the goals of the instrument.

5.4 EVALUATION

The evaluation of the instrument was done by letting parents from School X respond to the questionnaire. Their answers were analysed thoroughly to determine the shortcomings of the tool and determine ways to improve it. Interviews were conducted with some parents after they completed the questionnaire. The feedback received from the questionnaire, as well as the results from the interviews, were analysed using thematic analysis and descriptive statistics.

The secondary school, School X, had 209 registered learners in 2016 when the research was conducted. Unfortunately, only about half of these learners' parents attended the meeting, and of those only 55 parents responded to the questionnaire. Among all responses, 48 of the questionnaires were usable.

The results from the qualitative data analysis are presented below. The detailed results of the questionnaire can be found in Appendix B.

5.4.1 Interview Results

The analysis of qualitative data using thematic analysis methodology resulted in four main themes: the desired *end-results* impact of an awareness campaign, the *cyber safety content* to be discussed during a campaign, the *constraints* or issues that one must keep in mind during the campaign and *parallel actions* that must be taken to increase the overall effectiveness of the campaign. Each theme has sub-themes presented in Table 8.

Table 8 Interview Results

Themes	Details
Desired end-results	Improved cyber safety guidance for children Efficient assistance in monitoring children regarding cyber safety Consistent enforcement of rules and policies provided by the school Increased parents' digital literacy Empowerment of parents in children's education Decreased vulnerability of children Increased responsible use of ICT within the community Increased openness and trust between children and parents
Content to be discussed	Harmful online behaviours Tips to monitor children Useful monitoring tools and anti-virus usage etc. Latest trends Predators websites
Issues – Constraints	Information given is not easy to understand and apply Lack of communication No follow-up sessions with parents Lack of resources to provide efficient awareness Lack of involvement of parents
Parallel Actions	Constant education of parents and teachers Evaluation of current knowledge to avoid repetition of already known information during training Share awareness session by the level of knowledge Use of different media like TV, radio to pass information about cyber safety awareness

Desired end-results:

These are characterised by what would like to be achieved after the campaign. Parents highlighted their expectations of such a campaign so that when planning the content to be shared, the coordinator ensures their needs are met. Parents would appreciate gaining more insight into the digital world and to be more empowered in their role. Parents would like to be taught when to raise the red flag and how to react, or when to calm down and

relax. Parents would like to be able to create mutual trust between them and their children and still be able to have an eye on their children's activities.

Content to be discussed:

The parents talked about the subjects they felt were compulsory to a campaign they would take part in. It is essential to know what the main subjects they need to hear about are in order to make the campaign pleasant and beneficial for them. Parents said they needed to hear about the latest online trends concerning online activities and behaviours, especially among children, and what is considered good or bad online behaviour, even for themselves. Parents also need a list of websites to be aware of, especially known predator websites. Parents would like to be educated on tools one might use to monitor their children's online activities, without them feeling watched or pressured.

Issues – Constraints:

Parents emphasised the issues that may restrict the efficacy of the campaign so that the coordinators of the campaign keep them in mind and try to mitigate them. Even though the campaign is initiated, parents noted that if they are not sufficiently involved, the campaign will not be a success. Furthermore, the coordinator needs to make sure that the depth of the information given is aligned with their initial knowledge and current digital literacy. Parents would not appreciate that the training used too much jargon or technical words. The aim is to enlighten them, not to confuse them more. The campaign also needs to be well advertised and communicated so parents will make sure they avail themselves for it. The lack of communication could result in them missing the campaign. The campaign should take place regularly and should be balanced because technology is continuously evolving, and parents do not want to be bombarded with information at once. If the information is given once-off, parents will not be aware of upcoming things and might forget what was taught during the campaign. Finally, yet most importantly, the school or the government needs to invest in the training, as the lack of resources, like finances, books, hardware and software, might limit the impact and efficiency of the campaign.

Parallel actions:

Parents highlighted the type of actions that need to be performed in conjunction with the campaign in order to increase its impact and efficiency among the community. The school

or the government need to make sure that the children are continuously updated through parents and teachers. The content of the campaign must be compiled according to the audience’s level of literacy. Informal tests must take place to ensure that the content is understood and can be applied easily. The test will also avoid redundancy in the content shared and will ensure the training is taken more seriously by parents. The campaign must reach different kinds of audiences. Thus, it should be translated in all the South African official languages and adapted to various media, like radio and television, and shared throughout.

5.4.2 Questionnaire Results

The analysis of the quantitative data using descriptive statistics resulted in the following findings. The major findings are detailed in Table 9 below. The findings are also linked to the components of our Cyber Safety Information Framework. Comprehensive results can be found in Appendix B.

Table 9 Results of the Cyber Safety Information Needs Assessment Instrument

Framework Components	Results
Governance	54% of parents do not know the school’s policy but know it exists.
Parents	66% need cyber safety information 75% are worried about their children’s cyber safety 50% are aware of the concept of cyber safety Children are all in secondary school therefore in the same age category 93% own a smartphone 34% think that they should be in charge of their children’s said their children possess a mobile device from the age of 10 but use the internet actively from the age of 14
Cyber Safety topics	Threats they are most aware of: Predators (85%) Malware/viruses (82%) Identity theft (79%) Cyberbullying (77%)
. Resources	Not included
Delivery	Most parents prefer information via a printed brochure (54%) 29% prefer online information

5.4.3 Revising the Cyber Safety Information Needs Assessment Instrument (CSINAI)

The results above have helped to update the questionnaire to create the final version of the CSINAI available for parents. Some questions have been removed, and others have been added to the instrument to augment its relevance and completeness.

The preliminary questionnaire consisted of several questions that were not straight to the point at the beginning, especially in the third section. The open-ended questions were too ambiguous, which lead some of the respondents not to answer them. These questions were reformulated. The respondents also complained about the length of the instrument. Since more questions were removed then added, the questionnaire was shortened.

The final version of the Instrument can be found in Appendix C.

5.4.4 How to Apply the Cyber Safety Information Needs Assessment Instrument (CSINAI)

To effectively apply the CSINAI, one needs to analyse the most recurring patterns of the answers in each on its sections. A “High”, “Medium” or “Low” code is assigned to each question, depending on how it was answered. Tables 10, 11 and 12 below provide the way the codes are assigned to each question from the different sections of the questionnaire.

One will define the value of each answer whether it is high, medium or low, to determine the ability of each parent.

The most recurring pattern will be considered as most likely to be applicable to the parents targeted by a specific campaign.

5.4.4.1 First Section: Digital Literacy

Table 10 Results Equivalent for Section 1

Question number	Response A (Often and sometimes)	B or Seldom	C/ Never or I don't know
1	High	Low	NA
2	High	Low	NA
3	High	Low	NA
4	Low	Medium	High
5	High	Medium	Low
6	High	Medium	Low
7	High	Low	Medium
8	High	Low	Medium
9	High	Low	Medium

Considering the Table 10 above, one may say that whenever “High” is a more recurrent pattern, it means that the parents are digitally literate, whenever it is “Medium”, the parents would only know the basics and with “Low”, they would know very little. It will be indicative of the level at which the information can be shared during the campaign.

5.4.4.2 Second Section: Cyber Safety awareness

Table 11 Results Equivalent for Section 2

Question number	Response A (Often and sometimes)	B or Seldom	C/ Never or I don't know
10	Low	Medium	High
11	Low	Medium	High
12	Low	Medium	High
13	Low	Medium	High
14	Low	Medium	High
15	Low	Medium	High
16	Low	Medium	High
17	Low	Medium	High
18	Low	Medium	High
19	Low	Medium	High
20	Low	Medium	High
21	High	Medium	Low

Considering the Table 11 above, the researchers may say that whenever “High” is a more recurrent pattern, it means that the parents are aware of the possible threats, whenever it is

“Medium”, the parents would only know the basics and with “Low”, they would know very little. Considering each threat will give an idea of which threats to emphasise on during the campaign.

5.4.4.3 Third section: Parents’ communication preference

Table 12 Results Equivalent for Section 3

Question number	Response A (Often and sometimes)	B or Seldom	C/ Never or I don’t know
22	Low	Medium	High
23	Low	Medium	High
24	Low	Medium	High
25	Low	Medium	High
26	N/A	N/A	N/A
27	N/A	N/A	N/A
28	Low	Medium	High
29	High	Medium	Low
30	N/A	N/A	N/A
31	N/A	N/A	N/A

Considering Table 12 above, one may say that whenever “High” is the more recurrent pattern, it means that the parents are not willing to be contacted often, whenever it is “Medium”, the parents are not sure of what they would prefer and with “Low”, parents would be willing to be contacted often. One would also know whether parents are aware of the governance policies or not.

According to the recurring patterns of questions 26 and 27, one would discover their preferred delivery time and methods. Questions 30 and 31 are only to allow parents to raise their opinion on the campaign and give more ideas to Edu X on where and how to improve their awareness, according to the parents themselves.

5.4.4.4 RESULTS ACCORDING TO SCHOOL X'S RESPONSES

Table 13 Application of Results of the Questionnaire Inspired by Table 9's Results

Framework Components	Results	Topics/Items to be included in Categorisation
Governance	Low	Provide clear policies from the government and school
Digital Literacy Level	Medium	Give monitoring and security software Teach about hacking, spam and phishing and spoofing
Cyber Safety level	Medium-High	Regular updates on the most relevant recurring threats in RSA among the youth Regular updates on slang and new criminals' behaviour
Delivery Method	Most parents prefer information via a printed brochure (54%). 29% prefers online information	Compile brochure Compile categorisation of useful online content
Delivery Time	Most parents prefer information via a printed brochure (54%). 29% prefers online information	Sent online or given to children to take home

Table 13 refers to the kind of information that should be shared during a cyber safety awareness campaign at School X. Edu X should concentrate on sharing information about the policies of the school and the government, as there seems to be a lack of communication in this regard.

Parents at School X are relatively digitally literate, but the researchers observed a big gap between the digitally literate and the digitally illiterate. Therefore, Edu X should still give them the necessary information in this regard, as well as the first session to ensure that everyone is on the same level.

Most parents interviewed were aware of cyber safety and their threats. Ideally, parents should not receive basic information at first, but more specific information according to their needs, as indicated in table 13. Parents should also be given follow-ups and updated information at regular intervals.

Parents at School X are not willing to attend several sessions, so information should be concise during the campaign. Information to be shared may also be sent to them online or using brochure or pamphlets.

5.5 SUMMARY

The chapter above detailed Sub-Cycle 1 of the development phase of our main cycle of the Design Science Research Methodology followed along the research. The above results also serve as input for the following Sub-Cycle 2.

6 DEVELOPMENT – SUB-CYCLE 2: CATEGORISATION OF EXISTING CYBER SAFETY INFORMATION FOR PARENTS AND UPDATED VERSION OF THE FRAMEWORK

6.1 DEVELOPMENT – SUB-CYCLE 2: CATEGORISATION OF EXISTING CYBER SAFETY INFORMATION FOR PARENTS

The development phase of Design Science research will help construct the actual solution to the gap discovered in the previous phases. This sub-cycle focuses on the development of Categorisation of Existing Cyber Safety Information for Parents.

6.1.1 Awareness

The result of the evaluation of the Cyber Safety Information Needs Assessment Instrument has emphasised that more than 66% of parents questioned need guidance on how to approach cyber safety with their children. In addition, the results revealed that there is a lack of communication about cyber safety from the school. Various studies also found that in order to carry out a cyber safety awareness campaign, relevant content needs to be compiled (de Lange and von Solms, 2012; Dlamini et al., 2011; von Solms and von Solms, 2014). Service providers also require such categorisation of information for their customers. Therefore, there is a need for an application or document to be shared with schools, service providers or parents where one will be able to find up to date information about important topics of cyber safety with ease. To do that, some categorisation of existing online cyber safety content is needed.

6.1.2 Suggestion

Since there exists ample online material on cyber safety for not only children, but also adults, the idea is to categorise existing material according to themes and ages of children (similar to the work done by von Solms and von Solms (2014)). The researchers decided to use the categories as suggested by von Solms and von Solms (2014) as a starting point and

enhance it with results from the questionnaire. The parents identified 'slang' and 'tools' as themes according to the needs highlighted in the suggestion phase of the main cycle. To develop relevant material, one needs to cover the following aspects: the parent's initial abilities and knowledge, media available and content to be included.

The analysis of the data collected from the parents at School X has revealed that parents preferred to receive printed brochures where they can have regular up-to-date information about cyber safety, as it will not put a strain on their busy schedules. Parents also preferred to be on South African platforms, to increase the relevance of the information. Reference to information about relevant topics should form part of the categorisation according to parents' current level of literacy and the age of their children.

6.1.3 Development

The categorisation is a collection of online South African sources, categorised according to predefined themes (also identified by parents). The sources chosen had simple information that everyone could understand, considering the mixed levels of computer literacy and the initial cyber safety awareness of parents.

The researchers decided to use the categories as suggested by von Solms and von Solms (2014) as a starting point and enhance it with results from the questionnaire. The parents identified the themes of 'slang' and 'tools'. The researchers populated the categorisation framework with essential website links. This instance of the categorisation is considered work-in-progress and the service provider can always add new links and resources. At this point, the categorisation of links is a subjective judgement to be made by the coordinator adding the link. The presentation type of the material referred to can be game cards, videos, books or websites (as was shown in the literature review). The categorisation framework can be adapted to the needs of the audience.

The categorisation framework is given below in table 14.

DEVELOPMENT – Sub-Cycle 2: Categorisation of Existing Cyber Safety Information for Parents and Updated Version of the Framework

Table 14 Categorisation Framework

Themes	Topic	Subtopics	Digital literacy level	Cyber Safety awareness level	Presentation type	Age group	Reference
Cyber Safety threats	Technology related threats	Hacking Malware Spyware					
	Content related threats	Exposure to illicit or inappropriate content					
	Harassment related threats	Cyber-bullying Cyber-stalking Sexting Predators Scam					
	Risk of exposing information	Phishing Social networks/social media					
Trends (newest trends)	Slang	Slang tips					
Tools	Monitoring Security Engagement with children	Monitoring Security Engagement with children					
Policies		School policies National policies					

DEVELOPMENT – Sub-Cycle 2: Categorisation of Existing Cyber Safety Information for Parents and Updated Version of the Framework

Themes	Topic	Subtopics	Digital literacy level	Cyber Safety awareness level	Presentation type	Age group	Link
Cyber Safety threats	Technology related threats	Hacking	med	med	online content	high school children	http://www.waxedmedia.co.za/digitaljungle/hacker_protection_and_cyber_crime_in_south_africa http://cybercrime.org.za/hacking/
		Malware	med	med	online content	high school children	http://sacfis.co.za/viruses.htm http://icode.org.za/home-why.php
		Spyware	med	med	online content	high school children	http://cybercrime.org.za/spyware/
	Content related threats	Exposure to illicit or inappropriate content	low-med	med	online content	high school children	https://saferinternetsouthafrica.co.za/prevent-downloading-malicious-app/ https://saferinternetsouthafrica.co.za/selfies-nudes/ https://saferinternetsouthafrica.co.za/inappropriate-websites/
	Harassment related threats	Cyber-bullying	med	med	online content	high school children	http://www.cyberbullying.org.za/cyberbullying-in-sa.html http://www.cyberbullying.org.za/uploads/2/7/8/4/27845461/online_abuse_-_adults.pdf https://saferinternetsouthafrica.co.za/topics/cyber-bullying/
		Cyber-stalking	med	med	online content	high school children	http://cybercrime.org.za/cyberstalking/ https://saferinternetsouthafrica.co.za/online-stalking/
		Sexting	med	med	online content	high school children	http://www.cyberbullying.org.za/sexting.html https://saferinternetsouthafrica.co.za/sexting/

DEVELOPMENT – Sub-Cycle 2: Categorisation of Existing Cyber Safety Information for Parents and Updated Version of the Framework

		Predators	low	low	online content	high school children	http://www.cyberbullying.org.za/online-enticement.html http://sacfis.co.za/idtheft.htm http://www.cyberbullying.org.za/child-pornography.html https://saferinternetsouthafrica.co.za/grooming/ https://saferinternetsouthafrica.co.za/online-strangers/
		Scam	low	med	online content	high school children	https://scambuster.co.za/ http://sacfis.co.za/sms.htm http://crimeweb.co.za/
	Risk of exposing information	Phishing	low	low	online content	high school children	https://www.youtube.com/watch?v=0XZzcorg2k4 https://saferinternetsouthafrica.co.za/phishing/
		Social networks/social media	low	low	online content	high school children	http://www.cyberbullying.org.za/being-safe-on-facebook.html http://www.cyberbullying.org.za/being-safe-on-twitter.html http://www.cyberbullying.org.za/being-safe-on-instagram.html http://www.cyberbullying.org.za/im-chat-rooms-and-email.html https://saferinternetsouthafrica.co.za/parents-guide-snapchat-keeping-kids-safe/ https://saferinternetsouthafrica.co.za/topics/social-media-guides/ https://saferinternetsouthafrica.co.za/online-dating/ https://saferinternetsouthafrica.co.za/online-chat/ https://saferinternetsouthafrica.co.za/social-media-networks/ http://www.cyberbullying.org.za/videos.html https://saferinternetsouthafrica.co.za/inappropriate-photographs/

DEVELOPMENT – Sub-Cycle 2: Categorisation of Existing Cyber Safety Information for Parents and Updated Version of the Framework

Trends (newest trends)	Slang	Slang	low	low	online content	high school children	http://www.mirror.co.uk/news/uk-news/alarmed-secret-sexting-trolling-codes-9583904
		tips	low	low		high school children	https://saferinternetsouthafrica.co.za/topics/safe-resources/ https://www.facebook.com/staysafeonline/southafrica https://alertafrica.com/awareness/ https://saferinternetsouthafrica.co.za/prevent-downloading-malicious-app/
Tools	Monitoring	Monitoring	med-high	med-high	software/application	high school children	https://www.kaspersky.co.za/safe-kids https://www.virtuenet.co.za/
	Security	Security	med-high	med-high	software/application	high school children	https://www.kaspersky.co.za/free-antivirus
	Engagement with children	Engagement with children	low	low	online content	high school children	http://sacfis.co.za/safetytips.htm http://www.cyberbullying.org.za/uploads/2/7/8/4/27845461/connected_dot_com_tip_sheet.pdf https://saferinternetsouthafrica.co.za/topics/parental-advice/
Policies		School policies	low	low	online content	high school children	to be provided by School X
		National policies	low	low	pdf	high school children	https://www.gov.za/sites/default/files/39475_gon609.pdf https://www.education.gov.za/Programmes/SafetyinSchools.aspx

Table 15 Categorisation According to School X Parents' Needs

DEVELOPMENT – Sub-Cycle 2: Categorisation of Existing Cyber Safety Information for Parents and Updated Version of the Framework

Several South African links have been categorised according to this framework and are given in table 15 above. The categorisation has been populated according to the results of the case study done on School X. The researchers used only South African links, as per parents' requests, and the type and depth of information have been chosen according to their specific needs.

6.2 DEVELOPMENT – MAIN CYCLE: UPDATED VERSION OF THE CYBER SAFETY INFORMATION FRAMEWORK

The development phase of Design Science research will help construct the actual solution to the gap discovered in the previous phases. This section will detail how the framework was updated according to the previous sub-cycles.

6.2.1 Introduction

The following section forms part of the development of the main cycle of the research. It will relate how (from the suggested components of the framework and the two previous sub-cycles) the Cyber Safety Information Framework has been updated accordingly.

6.2.2 Updated Cyber Safety Information Framework

From the information collected, the researchers realised that the preliminary framework needed to be updated. The framework now comprises three components: the Cyber Safety Information Needs Assessment Instrument (CSINAI), the Categorisation and the preliminary Cyber Safety Information Framework found in the main cycle suggestion phase in section 4.2. These three components are interconnected.

The preliminary Cyber Safety Information Framework provides the main topics to be looked at when planning a cyber safety awareness campaign. These topics will serve as guidelines for the campaign. The Cyber Safety Information Needs Assessment Instrument will be used initially when wanting to discover the prerequisites of the material to be compiled for the awareness campaign. The questions of the Cyber Safety Information Needs Assessment

DEVELOPMENT – Sub-Cycle 2: Categorisation of Existing Cyber Safety Information for Parents and Updated Version of the Framework

Instrument were compiled to provide more insight into the elements cited in the preliminary framework. Links from the Categorisation are the actual items and content that will be presented during the awareness campaign.

The final Cyber Safety Information Framework is shown in figure 24 below.

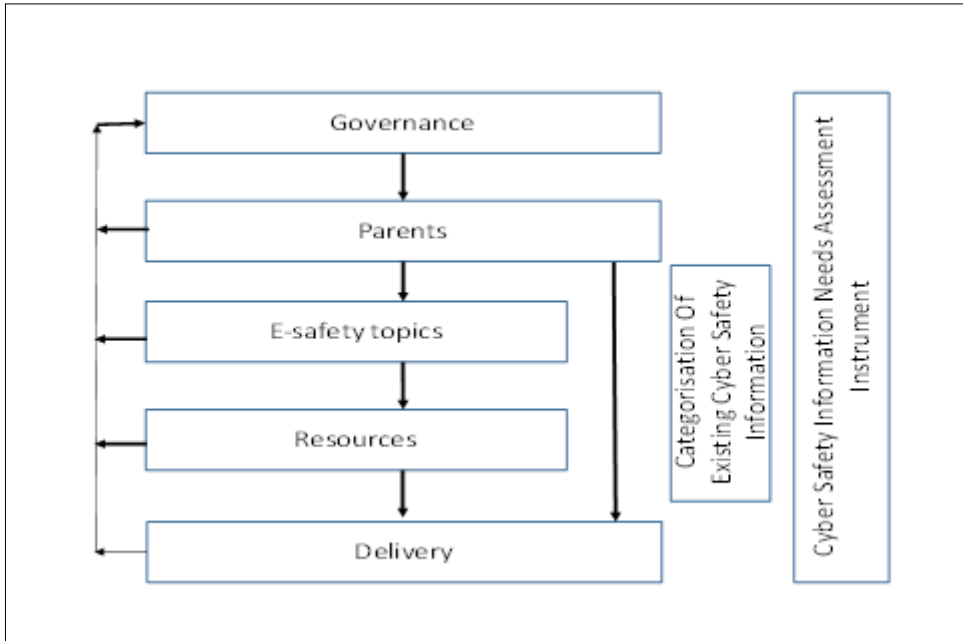


Figure 24 Updated Cyber Safety Information Framework

6.3 SUMMARY

The development phase of the Design Science Research Methodology has been divided into 2 Sub-Cycles to create a Cyber Safety Information Needs Assessment Instrument and Categorisation of Existing Cyber Safety Information for Parents. The Categorisation and the CSINAI have been developed to improve the quality and relevance of the final framework.

According to them, the framework has also been reviewed and updated.

The following will explain how the evaluation of the framework proceeded, as recommended in the Design Science Research Methodology.

7 EVALUATION – MAIN CYCLE

This chapter describes the Evaluation of the Cyber Safety Information Framework for parents. This was done by designing a prototype of a system based on the framework. For the purpose of this research, the prototype was not physically built. The design of the prototype was shown to a representative of Edu X during an interview session, to be evaluated according to some of the criteria proposed by Oates (2006). Her feedback was used to refine the framework and prototype system.

The approach used is discussed below.

7.1 THE APPLICATION OF THE CYBER SAFETY INFORMATION FRAMEWORK

Parents need to complete the questions in the instrument. The School will collect the answers to the questions, then send them to Edu X, along with the School's cyber safety policies, if any. Edu X will analyse the responses to find out the parents' preferences and needs. Once it has been discovered, the information will be entered in Edu X's application (Cyber Safety Awareness Form and database) design. The system will match the requirements of the specific school to their database of resources and compile the list of relevant resources according to the children's age group, the cyber safety awareness levels, digital literacy levels and communication preference. This list will then be sent back to the School, who will perform the cyber safety awareness training or run an awareness campaign for parents.

School X will share the CSINAI with the parents during a session (a parents' meeting, in our case), after which the school will send the results to the service provider (Edu X). Edu X then enters the details of the school and their needs according to their digital literacy and cyber safety awareness levels and communication preferences into the system, after which a list of possible cyber safety resources will be provided.

The following sections will detail the technology and approaches used to design the system.

7.1.1 Cyber Safety Awareness Form

The Cyber Safety Awareness Form has been designed using HTML, JavaScript, CSS and some PHP properties. It comprises the necessary elements needed to be collected in order to generate the categorisation.

Edu X will be entering information about the school such as their name, location, phone number and email for the record. One person will then enter the parents' cyber safety awareness and digital literacy levels, as well as the age of their children and their medium/communication preferences to pinpoint the topics and the levels of complexity of the information that will be provided in the categorisation.

It will also request whether the school has policies in place so that they can be included in the categorisation. The system will then check the matching resources in their database and generate a list of relevant links and information.

The preliminary chosen layout of the form is shown below.

Awareness form

Please enter the relevant Client's information needed below

School name:

Location:

Phone Number:

E-mail:

Cyber Safety awareness level

Low
 Medium
 High

Digital literacy level

Low
 Medium
 High

Age of children

5-12
 10-12
 12-15
 15-18

Interesting topics, you may select more than 1

- Technology Related
- Content Related
- Harassment Related
- Risk of Exposing Personal Info

Preferred type of resources, you may select more than 1

- hardcopy books
- electronic document
- Website
- Interactive Content

Does the client has cyber safety rules and policies already in place?

Yes, if yes include in categorisaion
 No

Figure 25 Preliminary Cyber Safety Awareness Form

7.1.2 Database

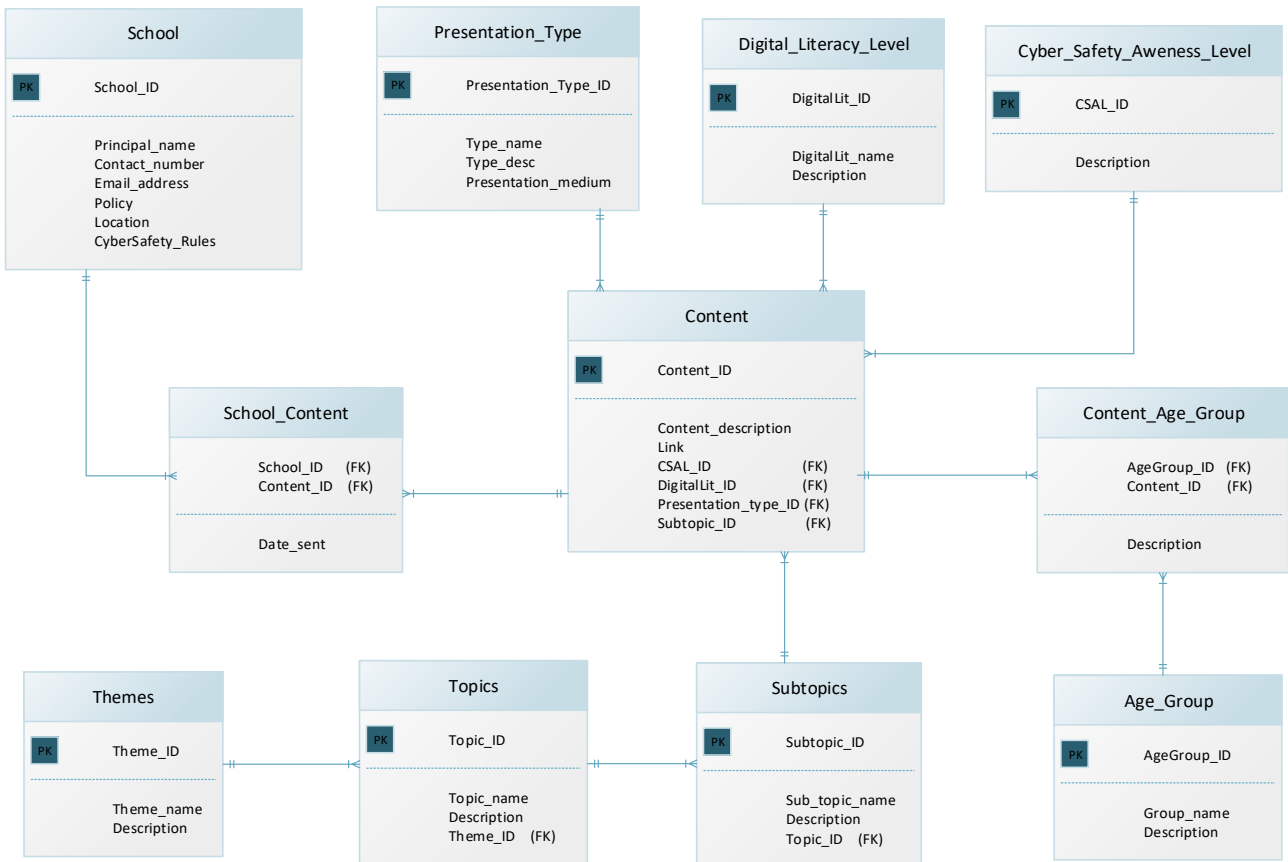
The underlying data model of this system is given below. The following tables are included:

- School: where relevant information of the school is stored
- Themes: where all the themes as described in Table 8 are stored
- Topics
- Sub-topics
- Age group: age groups 5 - 10, 10 – 12, 12 – 15, 15 -18

- Cyber Safety awareness levels: where the levels low, medium and high are stored. Each of these levels is determined according to the CSINAI. This is discussed in more detail in section 5.4.4
- Digital literacy levels: where the levels low, medium and high are stored. Each of these levels is determined according to the CSINAI. This is discussed in the section 5.4.3
- Presentation type: where the different kinds of presentations are stored. These include links, pdf, interactive content (games, activity cards), video, workbooks.
- Content: where the different resources (links, references) are stored.

The proposed database used to save information received from the Cyber Safety Awareness Form has been presented below using an ERD.

The ERD proposed below can be utilised, implemented and physically tested in further research.



7.2 EVALUATION FEEDBACK

7.2.1 Evaluation Criteria

To evaluate the framework, it, along with its instantiation, has been sent to a representative of Edu X who holds the position of training manager at Edu X. She was identified within the organisation as the best representative of Edu X for this study, due to her experience in the post and her extensive knowledge of the requirements a training session requires. She has trained parents, teachers, and children in schools and at church events. She reviewed the CSINAI, Cyber Safety Awareness Form, the ERD for the database, as well as the categorisation of online cyber safety content. An interview of 1.5 hours was conducted where she provided her feedback.

The evaluation criteria that were used for the envisaged system are given below:

- functionality (usefulness to their needs),
- usability (the ease of use),
- completeness,
- aesthetics and
- their expectation versus what the researchers have provided them

She also provided advice and possible improvements to be implemented to the system.

7.2.2 Feedback

The following feedback has been obtained from the representative of Edu X.

7.2.2.1 Cyber Safety Information Needs Assessment Instrument

- *Functionality (usefulness to their needs)*

- The Instrument was relevant and could be used in their activities.
 - o *Usability (the ease to use)*
- The Instrument is a bit long. However, nothing was irrelevant.
 - o *Completeness*
- It should be accompanied with a manual on how everything works and is interlinked for Edu X's use.
- A question about the age of children should be added in case the Instrument is not used in school environments only.
- All the essential topics were included in the document.
 - o *Aesthetics*
- Rewording was needed, especially in questions 4 and 9.
- Questions needed to be shortened to reduce the time parents spend filling out the instrument.
 - o *Their expectation vs what the researchers have provided them*
- The instrument reached their expectation and can be used in their activities.
 - o *Advice and Possible Improvements*
- A trainer should assist parents in the completion of the questionnaire to guide them through some of the more difficult and disturbing definitions of cyber safety threats.
- There should be a way to cancel some questions if other questions require a yes or no reply.

7.2.2.2 System (DATABASE + Cyber Safety Awareness Form)

- o *Functionality (usefulness to their needs)*
- The form is useful and relevant.
 - o *Usability (the ease to use)*
- The ERD is clean and easily implementable.
- The form is straight to the point and easy to use.
 - o *Completeness*
- The Form and the ERD were complete.
 - o *Aesthetics*
- Improve the layout – sections should follow each other in the Awareness Form.
- Rewording needs to take place in the Awareness Form.

- *Their expectation vs what the researchers have provided them*
- Such a system will meet their expectation.
- *Advice and Possible Improvements*
- She only advised improving the look and feel of the input form.

7.2.2.3 Categorisation of Existing Cyber Safety Information for Parents

- *Functionality (usefulness to their needs)*
- The Categorisation is clear and relevant.
- *Usability (the ease to use)*
- The categorisation is easy to understand and
- It is quickly compiled through the form which makes everything easier
- *Completeness*
- The categorisation was complete.
- *Aesthetics*
- Not applicable (this is only the information that will be used to populate part of the database).
- *Their expectation vs what the researchers have provided them*
- The categorisation met their expectation with the given content.
- *Advice and Possible Improvements*
- To propose functionality in the input form such that the complete categorisation can be shared with schools or parents if needed.
- To propose templates according to the chosen delivery medium.

7.2.2.4 Overall

She found the whole system potentially very useful and relevant to their needs, even though the user's Cyber Safety Awareness Form needs to be improved and the full development of the system has not been done yet.

Edu X's representative also appreciated the logic behind the Framework, especially the CSINAI and the Categorisation, and would like to see them used. The lady found all the outcomes/instantiation were good representations of the Framework and its utility; and

recommended its use for not only Edu X, but also other organisations that work toward the improvement of cyber safety awareness of the community.

7.2.3 Refinements

The refinements and improvements suggested by Edu X's representative were implemented as follows.

- A short user manual for the entire system, (see Appendix D) has been developed for Edu X.
- Rewording and aesthetics changes have been done on the CSINAI and on the Cyber Safety Awareness Form. Below is the final look of the Awareness form. The final version and details for both the CSINAI and the Awareness Form are to be found in Appendix E.

Cyber Safety Awareness Form

1. Please Enter the Relevant Client's Information Needed Below:

School Name:

Location:

Phone Number:

E-mail:

2. Please Rate the Parents' Cyber Safety Awareness Level:

Low
 Medium
 High

3. Please Rate the Parents' Digital Literacy Level:

Low
 Medium
 High

4. Please Select the Age Group of their Children:

5-10
 10-12
 12-15
 15-18

5. Please Select the Relevant Topics to be Included in the Categorisation, you may select more than 1:

Technology Related
 Content Related
 Harassment Related
 Risk of Exposing Personal Info

6. Please Select the Preferred Type of Resources, you may select more than 1:

Hardcopy Books
 Electronic Document
 Website
 Interactive Content

7. Would you like to Include the School's Policies to the Categorisation?

Yes
 No

Figure 27 Final Cyber Safety Awareness Form

7.3 CONCLUSION

The chapter above presented the Evaluation phase of the main cycle of the Design Science Research Methodology. It detailed how the evaluation of the framework took place.

The Framework has been instantiated into a design for a system comprising a Cyber Safety Awareness Form and a database design. This system was designed but not yet implemented and shared with Edu X, along with the CSINAI and the Categorisation. According to their feedback, the CSINAI and the Cyber Safety Awareness Form were updated. According to their recommendation, a manual has been compiled to use the CSINAI and system efficiently and, therefore, have an effective Cyber Safety Awareness campaign.

The following chapter is the last phase of the Design Science Research Methodology, namely the Conclusion phase, and will also conclude the research with future research and responses to the research questions. This chapter will summarise the responses to the research questions, detail the limitations of the study and propose future research. It will also relate how the outcomes of the research were shared with the public.

8 CONCLUSION – MAIN CYCLE

The following phase relates how and where the research questions were answered in the dissertation. It also gives details on how the framework was shared with the public and the contribution this made. This chapter will also specify the limitations of the studies, and propose future research which can arise from this study, as recommended in the Design Science Research Methodology.

8.1 RESPONSES TO RESEARCH QUESTIONS

This dissertation addressed a gap noticed in the South African context whereby the researchers realised that parents were not sufficiently equipped to assist their children with cyber safety awareness. In order to fill that gap, research questions were formulated. The following sections will explain how and where these questions were addressed in the dissertation.

8.1.1 Sub Research Questions

- *What are the cyber safety threats of using mobile devices, especially for learning purposes?*

The cyber Safety threats are, among others, cyberbullying, sexting, sharing of personal information, malware/virus and identity theft. These threats are explained and discussed in detail in section 2.5.1.

- *What is being done locally and internationally to make parents aware of cyber safety in schools and at home?*

The government initiated several actions in developed countries like the UK, USA and Canada. Unfortunately, Africa, with several developing countries, lacks infrastructure and regulations about cyber safety. In South Africa especially, actions are mostly initiated privately by schools or NGOs. Government and Schools should be more involved and should be responsible of the implementation of mobile learning and the framework. This is discussed in detail in sections 2.5.3 and 2.5.4.

- *What measures are being taken by schools in South Africa to inform parents about the cyber safety-related issues when they are implementing the use of mobile devices?*

Schools mostly rely on the service provider that will be implementing the changes to mobile learning. That is why Edu X needed material to help them sensitise parents about cyber safety awareness. However, some universities created associations that can visit schools to help with cyber safety awareness, as well. This is detailed in sections 2.5.2, 2.5.3 and 2.5.4.

- *How can the information's needs of parents be determined in the South African context regarding cyber safety awareness?*

The parents' cyber safety information needs can be determined using the CSINAI developed in this dissertation. The development process followed to obtain it can be found in Chapter 5. The final version is available in Appendix E.

- *How can existing cyber safety information be categorised to fulfil South African parents' needs?*

Cyber safety information available can be categorised using the Categorisation of Existing Cyber Safety Information for parents developed in the study. The process followed for the development of such categorisation can be found in Chapter 6. The actual Categorisation, along with its framework to be used generically, can be found in section 6.1.3.

- *What would an instantiation of the framework look like?*

The framework can be instantiated through an information system of which a preliminary Cyber Safety Awareness Form and database design were provided. The system's design was discussed in section 7.1.

In addition, the set-up for an effective cyber safety awareness campaign was discussed in section 7.2.2.

8.1.2 Main Research Question

How should a Cyber Safety Information Framework be formulated such that is relevant to the needs and expectations of parents?

A Cyber Safety Information Framework has been developed in this dissertation, and a preliminary version was produced in section 4.2; after which it was refined and further developed in Chapters 6 and 7. The final version of the framework is formulated as shown below. The framework was evaluated by collecting feedback from the intended user on its instantiation – a suggested design of an information system. The instantiation was refined, and a short user manual was provided for easier implementation of the system.

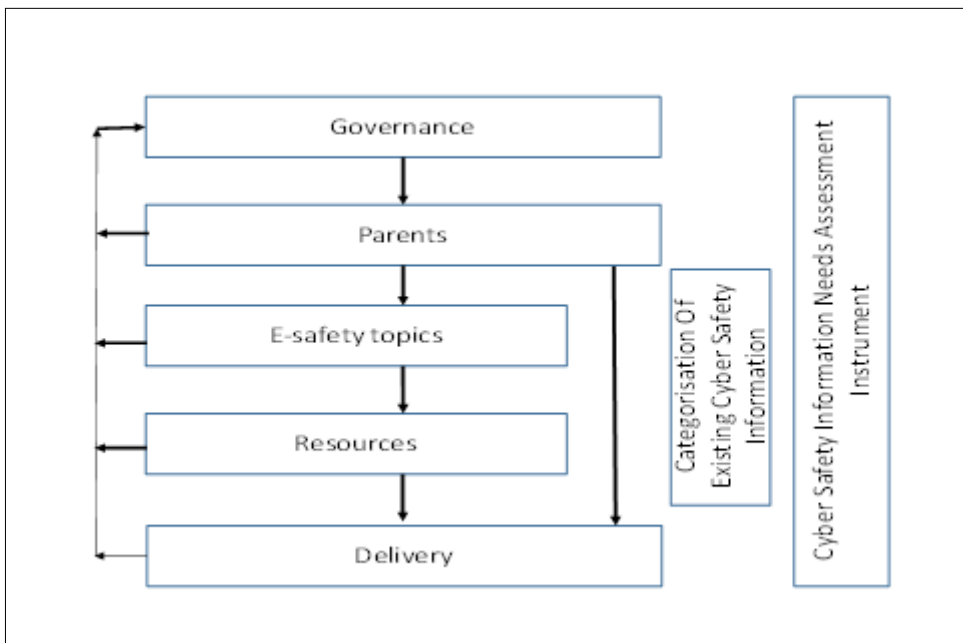


Figure 28 Final Version of the Cyber Safety Information Framework

8.2 LIMITATIONS

Limitations of a study are weaknesses that are present in research that cannot be changed (Simon, 2011). The limitations of this study are stated below.

- The results of the study might not be generalizable due to the size and the type of sample chosen. Therefore, since the sample chosen in this study comes from only one school with parents with an overall low level of cyber safety awareness and digital literacy, the results of the research might not apply to parents with a higher level of awareness and digital literacy.
- The results of the study might differ in a case where the school does not have policies and rules already in place. Before compiling the categorisation, a process should be added to assist schools and service providers to develop efficient and tailored rules and policies.
- The results of the study might have been influenced by the researcher's expectations and own feelings. However, in interpretive research, the assumption from which the researchers depart is that the researcher is subjectively involved in the research process.
- The criteria to analyse the results of the evaluation were subjectively chosen by the researcher.
- The analysis section can be automated in future research or by the customer if needed to reduce the time and possible human errors.

8.3 COMMUNICATION OF THE ARTEFACT AND FUTURE RESEARCH

As recommended in the methodology chosen for the study, the outcomes need to be shared with the public.

8.3.1 Communication of the Artefact

The final version of the Framework, accompanied with the CSINAI, the Categorisation framework, the populated categorisation, the system design guidelines along with an informal I walkthrough of the system, have been shared with Edu X in order for the school to be using them while implementing mobile learning in schools. Edu X also recommended the framework and the system should be shared with individuals who are involved in the Cyber Safety Awareness Campaign for the community so that it can assist them in their work.

The populated Categorisation of Cyber Safety Information for Parents has been shared with School X where the case study took place.

In addition, the first version of the framework has been presented at a conference in 2016: Paraiso, E. & Matthee, M., 2016. Towards a Cyber Safety Information Framework for South African Parents. Port Elizabeth, Nelson Mandela Metropolitan University, pp. 85-96.

8.3.2 Future Research

This research can be the starting point of several other studies in the field of cyber safety awareness. The system can be implemented and tested to evaluate if it really works in practice and an automation in the analysis of the results of the CSINAI can also be developed.

More extensive Evaluation form, CSINAI may be developed and tested.

The framework can also be tested differently and in different a setup. The framework might be used in other samples (teachers, school principals or government officials for example), communities, religious communities and universities – not only locally, but also internationally.

Further research may also look at how the framework may be adapted and applied on schools without policies in place.

Future research may even envision how to incorporate templates for the categorisation according to the chosen delivery methods. An evaluation of the progress of the parents through continuous training can be added to the framework and tested.

9 REFERENCES

African Centre of Excellence for Information Ethics, 2015. *A Toolkit For Digital Wellness*. [Online]

Available at: <http://www.up.ac.za/en/african-centre-of-excellence-for-information-ethics/article/2109737/digital-wellness-toolkit>

[Accessed 30 August 2017].

African Social Programmes and Initiatives, 2015. *Internet Safety Campaign*. [Online]

Available at: <http://iscafrica.net/#home>

[Accessed 1 July 2016].

Agatston, P. W., Kowalski, R. & Limber, S., 2007. Student's Perspectives on Cyber Bullying. *Journal of Adolescent Health*, Volume 41, pp. 59-60.

Akuta, E., Ong'oa, I. & Jones, C., 2011. Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice. *Journal of Peace, Gender and Development Studies*, 1(4), pp. 129-137.

Alhojailan, I. M., 2012. *Thematic Analysis: A Critical Review of Its Process and Evaluation*. Zagreb, Croatia, WEI International European, pp. 8-21.

Ally, M., 2004. *Using learning theories to design instruction for mobile learning devices*, London: Learning and Skills Development Agency.

Atkinson, S., Furnell, S. & Phippen, A., 2009. Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, 7(2009), pp. 13-19.

Australian Communications and Media Authority, 2010. *Cybersmart parents : Connecting parents with safety resources*, Melbourne: Commonwealth of Australia.

Australian Communications and Media Authority, 2015. *Parents' guide to online safety*.

[Online]

Available at:

http://www.cybersmart.gov.au/~media/Cybersmart/Documents/Documents/Parents_guide_to_online_safety.pdf

[Accessed 05 June 2015].

Australian Government, 2016. *Office of the Children's eSafety Commisser*. [Online]

Available at: <https://esafety.gov.au/education-resources/iparent>

[Accessed 03 August 2016].

Aycock, J., 2006. *Computer Viruses and Malware*. 1 ed. USA: Springer.

REFERENCES

- Bada, M. & Sasse, A., 2014. *Cyber Security Awareness Campaigns. Why do they fail to change behaviour?*, London: Global Cyber Security Capacity Centre.
- Badenhorst, C., 2011. Legal responses to cyber bullying and sexting in South Africa. *Centre for Justice and Crime Prevention*, August, Issue 10, pp. 1-20.
- Bamford, A., Powell, K. & Griffin, B., 2015. *Right Click: Parenting Your Teenager In A Digital Media World*. 1 ed. s.l.:Fuller Youth Institute.
- Bazon, E., 2013. *Why Do We Tolerate Revenge Porn?*. [Online]
Available at:
http://www.slate.com/articles/double_x/doublex/2013/09/revenge_porn_legislation_a_new_bill_in_california_doesn_t_go_far_enough.html
[Accessed 20 June 2016].
- Beger, G. & Sinha, A., 2012. *South African Mobile Generation : Study on South African young people on mobiles*, New York: UNICEF.
- Bell, D., Loader, B. D., Pleace, N. & Schuler, D., 2004. *Cyberculture: The Key Concepts*. s.l.:Taylor & Francis.
- Bell, M. A., 2002. *Kids can care about cyberethics!*, Norfolk, VA: Association for the Advancement of Computing in Education.
- Belsey, B., 2006. *Cyberbullying: An Emerging Threat to the "Always On" Generation*. [Online]
Available at: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf
[Accessed 16 June 2015].
- Bernard, H., 2002. *Research methods in anthropology: Qualitative and quantitative approaches*. 3rd ed. Walnut Creek, CA: Alta Mira Press.
- Bothma, T., 2015. *Digital Wellness Programme - ACTIVITY BOOK FOR SECONDARY SCHOOL LEARNERS*, Pretoria: African Centre of Excellence for Information Ethics.
- Boyatzis, R., 1998. *Transforming qualitative information: thematic analysis and code development*. Thousand Oaks: Sage Publications.
- Boyd, D., Marwick, A., Aftab, P. & Koeltl, M., 2009. The Conundrum of Visibility. *Journal of Children and Media*, 3(4), pp. 410-419.
- Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp. 77-101.
- Burns, N. & Grove, S. K., 2009. *The practice of nursing research: Appraisal, synthesis, and generation of evidence*, St. Louis, MO: Saunders Elsevier.

REFERENCES

- Burton, P. & Mutongwizo, T., 2009. Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. *Centre for Justice and Crime Prevention*, Issue 8, pp. 1-12.
- Byun, S. et al., 2009. Internet Addiction: Metasynthesis of 1996–2006 Quantitative Research. *CyberPsychology & Behavior*, 2(12), p. 203.
- Cabinet Office & The Rt Hon David Cameron MP, 2011. *Protecting and promoting the UK in a digital world*. [Online]
Available at: <https://www.gov.uk/government/news/protecting-and-promoting-the-uk-in-a-digital-world--3>
[Accessed 27 August 2015].
- Calluzzo, V. J. & Cante, C. J., 2004. Ethics in Information Technology and Software Use. *Journal of Business ethics*, Volume 51, pp. 301-312.
- Centers for Medicare & Medicaid Services (CMS), 2008. *Selecting a development approach*, USA: Office of Information Service - Department of Health and Human Services.
- Chigona, A., Chigona, W., Mpofo, S. & Bomkazi, N., 2009. *MXIT: Uses, Perceptions and Self-justifications*, Cape Town: University of Cape Town.
- Christodorescu, M. et al., 2005. *Semantics-Aware Malware Detection*. California, IEEE Xplore, pp. 32 - 46.
- Chua, W., 1986. Radical developments in accounting. *The Accounting Review*, 61(5), pp. 601-632.
- Citron, D. K. & Franks, M. A., 2014. Criminalizing Revenge Porn. *Wake Forest Law Review*, 49(2), pp. 345-392.
- Cole, K. et al., 2008. *Cybersecurity in Africa: An Assessment*, Atlanta: Georgia Institute of Technology.
- Cole, T. W., 1999. ACLU v. Reno : An exigency for cyberethics. *Southern Communication Journal*, 64(3), pp. 251-258.
- Computer Science and Telecommunications Board - National Research Council, 2002. *Youth , Pornography and the Internet*. Washington, DC: National Academy Press.
- Cranford, C., 2015. *Parenting in the Digital World: A Step-by-Step Guide to Internet Safety*. 1 ed. s.l.:CreateSpace Independent Publishing Platform.
- Cresswell, J. & Plano, C. V., 2011. *Designing and conducting mixed method research*. 2nd ed. Thousand Oaks, CA: Sage.

REFERENCES

- Creswell, J. W. & Plano Clark, V. L., 2007. *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage.
- Crosson-Tower, C., 2005. *Understanding child abuse and neglect*. Boston: Allyn & Bacon.
- CyberAngels; Time Warner Cable, 2007. *Cyber Safety Guide*, New York: The Alliance of Guardian Angels, Inc..
- Davison, R. M., 1998. *An Action Research Perspective of Group Support Systems:How to Improve Meetings in Hong Kong*, Hong Kong: City University of Hong Kong.
- de Joode, A., 2011. Effective Corporate security and cybercrime. *Network Security*, 3(2011), pp. 16-18.
- de Lange, M. & von Solms, R., 2012. *An e-Safety Educational Framework in South Africa*. Fancourt, George, SATNAC.
- Denning, P., 1991. *Computers under attack: intruders, worms, and viruses*. United States of America: Addison-Wesley Publishing.
- Denscombe, M., 2010. *The Good Research Guide: For Small-scale Social Research Projects*. 4th ed. Maidenhead: McGraw-Hill Education.
- Dictionary.com, 2015. *Awareness | Define Awareness at Dictionary.com*. [Online] Available at: <http://dictionary.reference.com/browse/awareness> [Accessed 08 June 2015].
- Dlamini, I., Taute, B. & Radebe, J., 2011. *Framework for an African Policy Towards Creating Cyber Security Awareness*. Gaborone, Council for Scientific and Industrial Research.
- Dlamini, M. T., Eloff, J. & Eloff, M., 2008. Information security: The moving target. *Computers & Security*, 28(2009), pp. 189-198.
- Dlamini, Z. & Modise, M., 2012. *Cyber Security Awareness Initiatives in South Africa: A Synergy Approach*. Seattle, Academic Publ. Internat.
- Dooley, J., Cross, D., Hearn, L. & Treyvaud, R., 2009. *Review of existing Australian and international cyber-safety research*, s.l.: ECU Publications Pre. 2011.
- Dorner, D. & Gorman, G., 2006. Information literacy education in Asian developing countries: cultural factors affecting curriculum development and programme delivery. *IFLA Journal*, 32(4), pp. 281-93.
- Duerager, A. & Livingstone, S., 2012. *How can parents support children's internet safety?*, London, UK: EU Kids Online.

REFERENCES

- Erasmus, J., 2015. *Identity theft in SA booming*. [Online]
Available at: <http://www.news24.com/SouthAfrica/News/Identity-theft-in-SA-booming-20150522>
[Accessed 2016 July 05].
- Eshet-Alkalai, Y., 2004. Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era. *Journal of Educational Multimedia and Hypermedia*, 13(1), pp. 93-106.
- Euro RSCG Worldwide, 2015. *This Digital Life*. [Online]
Available at: <http://mag.havas.com/prosumer-report/this-digital-life/>
[Accessed 10 November 2017].
- Faccio, E., Iudici, A., Costa, N. & Belloni, E., 2014. Cyberbullying and interventions programs in school and clinical setting. *Procedia - Social and Behavioral Sciences*, 112(2014), pp. 500-505.
- Freetutes, n.d. *Prototyping Software Life Cycle Model*. [Online]
Available at: <http://www.freetutes.com/systemanalysis/sa2-prototyping-model.html>
[Accessed 10 August 2016].
- Furnell, S. M. & Warren, M. J., 1999. Computer Hacking and Cyber Terrorism: The Reak Threat in the Millenium. *Computers and Security*, 18(1999), pp. 28-34.
- Gallaher, M. P., Link, N. A. & Rowe, R. B., 2008. *Cyber Security*. Cheltenham: Edward Elgar Publishing Limited.
- Gilliland, S., 2014. *Towards A Framework for Managing Enterprise Architecture Acceptance*, Vanderbijlpark: North West University.
- Gilster, P., 1997. *Digital Literacy*. New York: Wiley Computer Publishing.
- Government of Canada, 2013. *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, s.l.: Her Majesty the Queen in Right of Canada.
- Greenfield, R., 2013. *Why Isn't Revenge Porn Illegal Everywhere?*. [Online]
Available at: <http://www.thewire.com/technology/2013/08/why-isnt-revenge-porn-illegal-everywhere/68758/>
[Accessed 21 June 2016].
- Gregor, S. & Hevner, A. R., 2013. Positioning and presenting design science research for a maximum impact. *MIS Quaterly*, 37(2), pp. 337-355.
- Guba, E., 1990. *The paradigm dialog*. Ed ed. Thousand Oaks, CA, US: SAGE Publications.

REFERENCES

- Guba, E. & Lincoln, Y. S., 1994. Competing paradigms in qualitative research. In: N. Denzin & Y. Lincoln, eds. *Handbook of qualitative research*. 3rd ed. California: Sage, p. 105 – 117.
- Hanewald, R., 2008. Confronting the Pedagogical Challenge of Cyber Safety. *Australian Journal of Teacher Education*, 33(3), pp. 1-16.
- Heitner, D., 2016. *Screenwise: Helping Kids Thrive (and Survive) in Their Digital World*. 1 ed. s.l.:Routledge.
- Hevner, A. & Chatterjee, S., 2010. Evaluation. In: R. Sharda & S. VoB, eds. *Design Research in Information Systems: Theory and Practice*. New York: Springer, pp. 109-120.
- Hevner, A. R., 2007. A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, 19(2), pp. 87-92.
- Hevner, A. R., March, S. T., Park, J. & Ram, S., 2004. Design Science in Information Systems Research. *MIS Quarterly*, 28(1), pp. 75-105.
- Hollingworth, S. et al., 2009. *An exploration of parents' engagement with their children's learning involving technologies and the impact of this in their family learning experiences*, London: Becta.
- Huffaker, D., 2004. *Gender similarities and differences in online identity and language use among teenage bloggers*, Washington: researchgate.
- Hunton, P., 2011. A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, Issue 7, p. 105–113.
- Iivari, J. & Venable, J. R., 2009. *Action Research and Design Science Research: Seemingly similar but decisively dissimilar*. s.l., ECIS 2009 Proceedings, p. 73.
- iKEEPSAFE, 2016. *Cyber-Safety - iKEEPSAFE*. [Online]
Available at: http://ikeepSAFE.org/educators_old/more/c3-matrix/cyber-safety/
[Accessed 10 July 2016].
- Information and Communication Technology Services, 2013. *ICTS- It wasn't me!*. [Online]
Available at: <http://www.icts.uct.ac.za/modules.php?name=News&file=article&sid=6284>
[Accessed 02 July 2016].
- Internet Architecture Board, 1989. *RFC1087- Ethics and The Internet*, s.l.: University of Chicago Press.
- ISTQB Exam Certification, n.d. *What is Prototype model- advantages, disadvantages and when to use it?*. [Online]

REFERENCES

Available at: <http://istqbexamcertification.com/what-is-prototype-model-advantages-disadvantages-and-when-to-use-it/>

[Accessed 15 September 2015].

Jackman, T., 2016. *Sextortion, 'growing online problem worldwide, victimizes two George Mason students*. [Online]

Available at: <https://www.washingtonpost.com/news/true-crime/wp/2016/05/10/sextortion-growing-online-problem-worldwide-victimizes-two-george-mason-students/>

[Accessed 20 June 2016].

Jobi, T. & Kritzinger, E., 2014. *Online Awareness among Sepedi School*. Dublin, Ireland International Conference on Education (IICE-2014).

Johnson, L., Adams, S. & Cummins, M., 2012. *The NMC Horizon Report: 2012 Higher Education Edition*. Austin, Texas, The New Media Consortium.

Jugder, N., 2016. *The thematic analysis of interview data: an approach used to examine the influence of the market in curricular provision in Mogolian higher education institutions*, s.l.: Hillary Place Papers .

Kambourakis, G., 2013. Security and Privacy in m-Learning: Challenges and State-of-the-art. *International Journal of u- and e- Science*, 6(3), pp. 67-84.

Kivunja, C. & Kuyini, B., 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, 6(5), pp. 26-41.

Kong, S. C., 2008. A curriculum framework for implementing information technology in school education to foster information literacy. *Computer and education*, Volume 51, pp. 129-141.

Kong, S. C. & Li, K. M., 2008. Collaboration between school and parents to foster information literacy: Learning in the information society. *Computer and Education*, 52(2009), pp. 275-282.

Kortjan, N. & von Solms, R., 2013. Cyber Security Education in Developing Countries: A South African Perspective. In: K. Jonas, I. A. Rai & M. Tchunte, eds. *e-Infrastructure and e-Services for developing countries*. Yaounde: Springer, pp. 289-297.

Kortjan, N. & von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. *SACJ*, Issue 52, pp. 29-41.

Kowalski, R. M., Limber, S. P. & Agatston, P. W., 2012. *Cyberbullying: Bullying in the Digital Age*. 2nd ed. Malden, MA: Wiley-Blackwel.

REFERENCES

- Kritzinger, E., 2014. *Online safety in South Africa – a cause for growing concern*. Pretoria, ISSA.
- Kritzinger, E., 2015. *Enhancing Cyber Safety Awareness among School Children in South Africa through Gaming*. London, UK, Science and Information Conference.
- Kritzinger, E. & Padayachee, K., 2013. *Engendering an e-safety awareness culture within the South African context*. Pointe-Aux-Piments, 2013 Africon, pp. 1-5.
- Kritzinger, E. & von Solms, S., 2012. A Framework for Cyber Security in Africa. *Journal of Information Assurance & Cybersecurity*, 2012(2012), pp. 1-10.
- Ktoridou, D., Eteokleous, N. & Zahariadou, A., 2012. "Exploring parents' and children's awareness on internet threats in relation to internet safety. *Campus-Wide Information Systems*, 29(3), pp. 133-143.
- Kuhn, T., 1962. *The Structure of Scientific Revolutions*. 1st ed. Chicago: The University of Chicago press.
- Lee, A. P., 2010. *Cyberethics in Action : Copyrights, Privacy, and Awareness Teacher's Guide*, Kingston, Ontario: Queen's University.
- Leedy, P. & Ormrod, J. E., 2010. *Practical Research: Planning and Design*. 9th ed. NYC: Meryl.
- Lenhart, A., Madden, M. & Hitlin, P., 2005. *Teens and Technology: Youth are Leading the Transition to a Fully Wired and Mobile Nation*, Washington, D. C.: Pew Internet & American Life Project.
- Levesque, R., 1999. *Sexual Abuse of Children: A Human Rights Perspective*. Bloomington: Indiana University Press.
- Li, H. et al., 2018. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing*, 15(4), pp. 646-660.
- Livingstone, S. & Bober, M., 2005. *UK children go online*. London: London School of Economics.
- Looi, C., Sun, D. & Xie, W., 2014. Exploring Students' Progression in an Inquiry Science Curriculum Enabled by Mobile Learning. *Learning Technologies, IEEE Transactions*, 8(1), pp. 43-54.
- Ludwig, M., 1998. *The giant black book of computer viruses*. Show Low, Arizona: American Eagle.

REFERENCES

- Lynch, M., 1994. *Ethical issues in electronic Information Systems*, Austin: Department of Geography, University of Texas at Austin.
- Maifarth, M., Griesbaum, J. & Kölle, R., 2013. *Mobile Device Usage in Higher Education Available from:*, Frankfurt: University of Frankfurt.
- Makinen, O. & Naarmala, J., 2006. *Defining Cyberethics*, Vaasa: s.n.
- March, S. T. & Smith, G. F., 1995. Design and Natural Science research on Information technology. *Decision Support Systems*, 15(1995), pp. 151-166.
- Martin, F. & Ertzberger, J., 2013. Here and now mobile learning: An experimental study on the use of mobile technology. *Computers & Education*, 2018(68), pp. 76-85.
- Mason, R. O., 1995. Applying ethics to Information Technology issues. *Communication of the ACM*, 38(12), pp. 55-57.
- Matthee, M. C., Hattingh, M. J. (. & Weilbach, E. H. (., 2017. *The perception of South African parents on the use of technology in schools*, Pretoria: University of Pretoria (Informatics).
- Merriam Webster , 2019. *Need | Definition of Need by Merriam Webster*. [Online] Available at: <https://www.merriam-webster.com/dictionary/need> [Accessed 22 January 2019].
- Miles, M. & Huberman, A., 1994. *Qualitative Data Analysis*. 2nd ed. Thousand Oaks, CA: Sage Publications.
- Moore, J. H., 1985. What is computer ethics. *Methaphilosophy*, 4(16), pp. 266-275.
- Mossberger, K., Tolbert, C. J. & McNeal, R. S., 2008. *Digital Citizenship : The Internet, Society, and Participation*. Chicago: MIT Press.
- Mouton, J., 2001. *How to succeed in your master's and doctoral studies : A South African guide and resource book*. Pretoria: Van Schaik.
- Mukherjee, T. T., 2012. Online Research Methodology: Using the Internet and the Web for Research and Publication. *Bhatter College Journal of Multidisciplinary Studies*, Volume 2, pp. 55-65.
- Munro, E., 2011. *The protection of children online: a brief scoping review to identify vulnerable groups*, London: Childhood wellbeing research centre.
- Myers, M. D., 2013. *Qualitative Research in Business and Management*. 2 ed. s.l.:Sage.
- Naidoo, T., Kritzinger, E. & Looock, M., 2014. *Cyber Safety Education: Towards a Cyber-Safety Awareness. Framework for Primary Schools*. Cape Town, Cape Peninsula University of Technology, pp. 272-281.

REFERENCES

- Nambiro, A. W., Muchiri, G. M. & Matoke, N., 2014. Survey of Cyber Security Frameworks. *International Journal of Technology in Computer Science & Engineering*, 2(1), pp. 33-39.
- O'Connell, M. E., 2012. Cyber Security without Cyber War. *Journal of Conflict & Security Law*, 2(17), pp. 187-209.
- Oates, B., 2006. *Researching information systems and computing*. London, UK: SAGE.
- Ogundeji, O. A., 2014. *African organizations lag in cybersecurity, global survey says*. [Online]
Available at: <http://www.pcworld.com/article/2846312/african-organizations-lag-in-cybersecurity-global-survey-says.html>
[Accessed 20 August 2015].
- Onwuegbuzie, A. J. & Teddlie, C., 2007. A framework for analysing data in mixed methods research. In: A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and* . Thousand Oaks, CA: Sage, pp. 351-383.
- Padayachee, K., 2011. *Teaching safe and secure usage of ICT: A South African perspective*, Pretoria: University of South Africa.
- Paraiso, E. & Matthee, M., 2016. *Towards a Cyber Safety Information Framework for South African Parents*. Port Elizabeth, Nelson Mandela Metropolitan University, pp. 85-96.
- Patchin, J. W. & Hinduja, S., 2011. Traditional and Nontraditional Bullying Among Youth: A Test of General Strain Theory. *Youth and Society*.
- Peppers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), pp. 45-78.
- Pew Research Center, 2014. *Online Harassment*. [Online]
Available at: <http://www.pewinternet.org/2014/10/22/online-harassment/>
[Accessed 20 June 2016].
- Pollara, P., 2011. *Mobile learning in higher education: A glimpse and a comparison of student and faculty readiness/ attitudes and perception.*, Louisiana: Louisiana State University.
- Popovac, M. & Leoschut, L., 2012. Cyber bullying in South Africa: impact and responses. *Center for Justice and Crime Prevention*, Issue 13, pp. 1-16.
- Pries-Heje, J., Baskerville, R. & Venable, J. R., 2008. *Strategies for Design Science Research Evaluation*. Galway, Ireland, ECIS 2008.

REFERENCES

- Pruitt-Mentle, D., 2000. *The C3 framework: Cyberethics, cybersafety and cybersecurity implications for the educational setting*, s.l.: iKeepSafe.
- Pusey, P. & Sadera, W. A., 2011. Cyberethics, Cybersafety, and Cybersecurity. *Journal of Digital Learning in Teacher Education*, 28(2), pp. 82-88.
- Ramzan, Z., 2010. Phishing attacks and countermeasures. In: M. & S. P. Stamp, ed. *Handbook of Information and Communication Security*. s.l.:Springer.
- Republic of South Africa, 2007. *Criminal Law (Sexual Offences and Related Matters) Amendment Act*, s.l.: Government gazette.
- Resnik, D. B., 2011. *what is ethics in research and why is it important?*. [Online] Available at: <http://www.niehs.nih.gov/research/resources/bioethics/whatis/> [Accessed 20 May 2015].
- Ribble, M., 2015. *Digital Citizenship*. [Online] Available at: www.digitalcitizenship.net [Accessed 01 June 2015].
- Roddel & V., 2011. *The Ultimate Guide to Internet Safety*. 2nd ed. s.l.:Lulu Press.
- Rouse, M., 2010. *What is cybersecurity? - Definiton of WhatIs.com*. [Online] Available at: <http://whatis.techtarget.com/definition/cybersecurity> [Accessed 08 June 2015].
- Rusell, D. & Gangemi, G., 1991. *Computer security basics*, United Stataed of America: O'Reilly & Associates, Inc.;
- SA Health, 2013. *Cyber safety - Parent Easy Guide (PEG) - pegs 63*. [Online] Available at: <http://www.parenting.sa.gov.au/pegs/peg63.pdf> [Accessed 2nd November 2015].
- Sabella, R., Patchin, J. W. & Hinduja, S., 2013. Cyberbullying myths and realities. *Computers in Human Behavior*, 29(2013), pp. 2703-2711.
- SAPS, n.d. http://www.saps.gov.za/child_safety/teens/internet_safety. [Online] Available at: http://www.saps.gov.za/child_safety/teens/internet_safety.php [Accessed 2 July 2016].
- Selwyn, N., 2008. A Safe Haven for Misbehaving? An Investigation of Online Misbehavior Among University Students. *Social Science Computer Review*, 4(26), p. 446–465.
- Sharples, M., 2006. *Big issues in Mobile Learning. Report Of worshop by Kaleidoscope Network of Excellence Mobile Learning Initiative*, Nottingham: Kaleidoscope.

REFERENCES

- Shonola, S. A. & Joy, M. S., 2014. *Mobile Learning Security Concerns from University students' Perspectives*. Thessaloniki, Greece, IEEE, pp. 165-172.
- Simon, M. K., 2011. *Dissertation and scholarly research: Recipes for success*, Seattle, WA: Dissertation success, LLC.
- Social Security Administration, 2018. *Identity Theft and Your Social Security Number*, Washington: US GOV.
- Sonck, N., Livingstone, S., Kuiper, E. & de Haan, J., 2011. *Digital literacy and safety skills*, London, UK: EU Kids Online, London School of Economics & Political Science.
- Sonhera, N., Kritzinger, E. & Loock, M., 2012. *A Proposed Cyber Threat Incident Handling Framework for Schools in South Africa*. New York, ACM, pp. 374-383.
- South African Cyber Security Academic Alliance, 2016. *South African Cyber Security Academic Alliance | Cyber security for all South Africans*. [Online] Available at: <http://www.cyberaware.org.za/> [Accessed 1 July 2016].
- Stallings, W., 2012. *Computer security : principles and practice*. Boston: Pearson.
- Standing Council of Education and Early Childhood, 2010. *National Safe Schools Framework*, Carlton South: Education Services Australia.
- Statistics Canada, 2009. *Quality Guidelines*, s.l.: Minister of Industry.
- Sukhai, N. B., 2004. *Hacking and Cybercrime*. New York, ACM, pp. 128-132.
- Sun, Y. & Kantor, P. B., 2006. Cross-Evaluation: A new model for information system evaluation. *Journal of the American Society for Information Science and Technology*, 57(5), pp. 614-628.
- Symantec, 2013. *2013 Norton Report*, s.l.: Symantec.
- Tavani, H., 2004. *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Danvers Mass: Wiley & Sons.
- Telstra Corporation Limited, 2014. *Addressing the cyber safety challenge: from risk to resilience*. Sydney: Telstra Corporation Limited.
- The Federal Bureau of Investigation, 2015. *FBI - What is Sextortion?*. [Online] Available at: <https://www.fbi.gov/news/videos/what-is-sex-tortion/view> [Accessed 20 June 2016].
- Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E., 2005. The insider threat to information systems and the effectiveness of ISO 17799. *Computers and Security*, Issue 24, pp. 472-484.

REFERENCES

- Traxler, J., 2010. Will student devices deliver innovation, inclusion, and transformation?. *Journal of the Research Center for Educational Technology*, 6(1), pp. 3-15.
- Tsai, J., Kelley, P., Cranor, L. & Sadeh, N., 2010. *Location-Sharing Technologies: Privacy Risks and Controls*, Pittsburgh, PA: Carnegie Mellon University.
- Uhls, Y., 2015. *Media Moms & Digital Dads: A Fact-Not-Fear Approach to Parenting in the Digital Age*. 1 ed. s.l.:Routledge.
- UK Safer Internet Centre, 2016. *UK Safer Internet Centre*. [Online]
Available at: <http://www.saferinternet.org.uk/safer-internet-day/2016/parents>
[Accessed 01 August 2016].
- US Department of Justice, 2006. *Transcript of Attorney General Alberto R. Gonzales' Address to the Employees at the National Center for Missing and Exploited Children*. [Online]
Available at: https://www.justice.gov/archive/ag/speeches/2006/ag_speech_0604202.html
[Accessed 20 March 2016].
- US Department of Justice, 2016. *The National Strategy for Child Exploitation Prevention and Interdiction - A REPORT TO CONGRESS*, Washington: US Department of Justice.
- US National Center for Missing & Exploited Children, 2016. *Netsmartz Workshop | Parents & Guardians*. [Online]
Available at: <http://www.netsmartz.org/Parents>
[Accessed 29 July 2016].
- Vaishnavi, V. & Kuechler, B., 2004. *Design Science in Information systems*. [Online]
Available at: <http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf>
[Accessed 10 June 2015].
- Vaishnavi, V. & Kuechler, W., 2007. *Design science research methods and patterns: innovating information and communication technology*. Boca Raton, FL: Auerbach Publications.
- Valcke, M., De Wever, B., Van Keer, H. & Schellens, T., 2011. Long-term study of safe Internet use of young children. *Computers & Education*, Volume 57, pp. 1192-1305.
- van Niekerk, J., Thomson, K. L. & Reid, R., 2013. Cyber Safety for School Children : A Case Study in the Nelson Mandela Metropolis. In: L. Fitcher & D. C. Dodge, eds. *Information assurance and Security - Education and Training* . Berlin Heidelberg: Springer , pp. 103-112.

REFERENCES

- Vanderbosh, H. & Van Cleemput, K., 2008. Defining Cyberbullying: A Qualitative Research into the Perceptions of Youngsters. *Cyberpsychology and Behavior*, 11(4), pp. 499-503.
- Vecchiato, P., 2005. *SADC Looking to Harmonise Cyber Laws*. [Online]
Available at:
http://www.itweb.co.za/index.php?option=com_content&view=article&id=122017:sadc-looking-to-harmonise-cyber-laws&catid=69:business
[Accessed 25 August 2015].
- Venable, J., 2006. A Framework for Design Science Research Activities. In: M. Khosrow-Pour, ed. *Emerging Trends and Challenges in Information Technology Management*. Hershey, PA: Idea Group Inc, pp. 184-187.
- Venable, J., 2011. Incorporating Design Science Research and Critical Research Into an Introductory Business Research Methods Course. *The Electronic Journal of Business Research Methods*, 9(2), pp. 119-129.
- Voigt, T. & Matthee, M., 2012. *Tablets with Restricted Mobility: Investigating User Acceptance in a South African Mathematics Mobile Learning Project*. s.l., mLearn, pp. 172-179.
- Volker, T., 2007. *Security goes from tactical to strategic*. [Online]
Available at: <http://mydl.itweb.co.za/>
[Accessed 15 August 2015].
- vom Brocke, J. & Buddendick, C., 2006. *Reusable Conceptual Models – Requirements Based on the Design Science Research Paradigm*. Claremont, CA, CGU.
- von Solms, A. & von Solms, R., 2014. *Towards a Cyber Safety Education in Primary schools in Africa*. Plymouth, UK, HAISA 2014, pp. 185-197.
- von Solms, R., 2011. *Children at risk of online bullying | Education | M&G*. [Online]
Available at: <http://mg.co.za/article/2011-02-04-children-at-risk-of-online-bullying>
[Accessed 16 June 2015].
- von Solms, R. & von Solms, S., 2015. Cyber Safety Education in Developing Countries. *SYSTEMICS, CYBERNETICS AND INFORMATICS*, 13(2), pp. 14-19.
- Wahyuni, D., 2012. The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies. *JAMAR*, 10(1), pp. 69-80.

REFERENCES

- Weilbach, L. & Matthee, M. C., 2015. Using the PSIC Model to Understand Change in an Educational Setting: The Case of an E-Textbook Implementation. *ECIS 2015 Completed Research Papers*, p. Paper 130..
- WEROBOT, 2017. *Hey Teens: Chances Are You'll Regret Oversharing Information Online*. [Online]
Available at: <https://www.webroot.com/us/en/home/resources/tips/digital-family-life/hey-teens-chances-are-youll-regret-oversharing-information-online>
[Accessed 10 november 2017].
- Winkler, I., 2005. . *Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day*. s.l.:John Wiley & Sons.
- Young, K., 1999. Internet addiction: Symptoms, evaluation and treatment. In: L. VandeCreek & T. L. Jackson, eds. *Innovations in Clinical Practice*. Sarasota, FL: Professional Resource Press.
- Youth Online Safety Working Group, 2010. *Interdisciplinary Response to Youth Sexting*, Rohnert Park, CA: s.n.
- Zainal, Z., 2007. Case study as a research method. *Jurnal Kemanusiaan*, Volume 9, pp. 1-6.

10 APPENDICES

10.1 APPENDIX A: QUESTIONNAIRE AND ETHICS APPROVAL



Faculty of Engineering,
Built Environment and Information Technology

1956 – 2016
60
years of
Engineering Education

Reference number: EBIT/23/2016

10 June 2016

Ms EL Paraiso
Department of Informatics
School of Information Technology
University of Pretoria
Pretoria
0028

Dear Ms Paraiso,

FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Research Ethics Committee refers.

Approval is granted for the application with reference number that appears above.

1. This means that the research project entitled "Cyber safety framework for South African parents" has been approved as submitted. It is important to note what approval implies. This is expanded on in the points that follow.
2. This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Code of Ethics for Scholarly Activities of the University of Pretoria, or the Policy and Procedures for Responsible Research of the University of Pretoria. These documents are available on the website of the EBIT Research Ethics Committee.
3. If action is taken beyond the approved application, approval is withdrawn automatically.
4. According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of the EBIT Research Ethics Office.
5. The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.

Prof JJ Hanekom
Chair: Faculty Committee for Research Ethics and Integrity
FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

EBIT Research Ethics Committee
Room 15-6, Level 15, Engineering Building 1
University of Pretoria, Private Bag X20
Hatfield 0028, South Africa
Tel +27 (0)12 420 3736
Email mar.ferreira@up.ac.za

Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie
Lefapha la Boetšenere, Tikologo ya Kago le Theknološhi ya Tshedimošo

Good day,

My name is Elvira L. Paraiso.

I am a student at the University of Pretoria (Student Number 15260772).

I am currently doing my Master's degree in Information Technology (Information Systems).

My study titled TOWARDS A CYBER SAFETY INFORMATION FRAMEWORK FOR SOUTH AFRICAN PARENTS is about the parents' awareness of cyber safety issues encountered online by their children especially. It aims to produce a material tailor made for parents to assist them in the safe online behaviour education of their children.

The following questionnaire will assist in my data collection.

Please be aware that your personal information will not be kept, and your confidentiality will be protected at any time while participating in this study.



Informed Consent Form

- 1 Title of research project: TOWARDS A CYBER SAFETY INFORMATION FRAMEWORK FOR SOUTH AFRICAN PARENTS
- 2 I hereby voluntarily grant my permission for participation in the project as explained to me by Elvira L. Paraiso.
- 3 The nature, objective, possible safety and health implications have been explained to me, and I understand them.
- 4 I understand my right to choose whether to participate in the project and that the information furnished will be handled confidentially.
- 5 I am aware that the results of the investigation may be used for the purposes of publication.
- 6 Upon signature of this form, you will be provided with a copy.

Signed: _____ Date: _____

Witness: _____ Date: _____

Researcher: _____ Date: _____

Questionnaire

Please cross (X) what applies to you.

Section 1

The first section will help determine the level of comfort you have with a computer/ mobile device and the internet.

1. Do you own a personal computer?
 - a) Yes
 - b) No

2. Do you own a smartphone/cellphone?
 - a) Yes
 - b) No

3. Do you own a tablet?
 - a) Yes
 - b) No

4. How often do per day you use your mobile device(s) (e.g. tablet, smartphone, personal computer)?
 - a) From 0 to 3 hours
 - b) From 3 to 8 hours
 - c) More than 8 hours

5. If yes from question 1, 2 or 3, you use the following apps/functionalities on your devices:

	Often	Sometimes	Seldom	Never	I do not know what it is
Instant messaging (e.g. WhatsApp, Mxit, Skype, BBM)					
SMS					
Web camera					
Voice notes					
E-mail					
Online Banking					
Reading news					
Social media (e.g. Facebook, Twitter, YouTube, Instagram)					
Search Engines (e.g. Google, Yahoo! Bing!)					
Gaming apps (e.g. Candy Crush Saga, Pet Rescue Saga)					

6. You are aware of the following:

	Yes and I have used it before	Yes but I have not used it	No
Changing privacy setting of mobile devices, websites and apps			
Changing preferences for mobile devices, websites, and apps.			
Blocking unwelcome adverts, popup messages			
Antivirus software			
Deleting website download history?			
Installing/uninstalling applications			

7. From what age is your child allowed to possess a mobile device (tablet, smartphone)?
 - a) Between 7 years old and 10 years old
 - b) Between 10 years old and 14 years old
 - c) From 14 years old and older

8. From what age is your child allowed to be on social media and browse the internet on its own?
 - a) Between 7 years old and 10 years old
 - b) Between 10 years old and 14 years old
 - c) From 14 years old and older

9. What is your feeling with your child being online?
 - a. I don't feel safe with my child being online
 - b. I don't have any concern

Section 2:

In each of the following questions, a concept is defined after which you need to indicate your level of awareness of the concept.

10. **Cyber safety** (the wise and responsible use of the internet and technology devices like tablets, and cellphones to be and remain safe online)
 - a) I have never heard about this before
 - b) I have heard of it, but I am not so familiar with this concept
 - c) I am fully aware of the concept and what it implies

11. **Sexting** (the sending and receiving photos or videos where the individuals are naked or partially naked. It also includes sexually suggestive messages sent through text messages or instant messaging).
 - a) I have never heard about this before
 - b) I have heard of it, but I am not so familiar with this concept
 - c) I am fully aware of the concept and what it implies

12. **Cyber bullying** (the use of the internet and technology devices to harass, discriminate and disclose someone's personal information. It is very common among children and can be very devastating.)
 - a) I have never heard about this before
 - b) I have heard of it, but I am not so familiar with this concept
 - c) I am fully aware of the concept and what it implies

13. **Internet** (through which children can access harmful content like pornography, hate speech or through which your device can be infected with viruses or malware).
 - a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies

14. **Predators** (People, paedophiles who exploit and manipulate children via the internet).
 - a) I have never heard about them before
 - b) I have heard of it, but I don't know how to recognise them
 - c) I am fully aware of it and what it implies

15. **Identify theft** (Personal information like identity, pictures shared online on social media or chat-room can be stolen or misused by individuals online).
 - a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies

16. **Location sharing** (People are often geo-tagging themselves to give parents/friends their location. The location sharing option can often be used by predators/stalkers to monitor them).
 - a) I have never heard about this before



- b) I have heard of it, but I don't know the extent
- c) I am fully aware of it and what it implies

17. Sharing of personal information (People especially children tend to share more than they should online like their address, real name, and habits).

- a) I have never heard about this before
- b) I have heard of it, but I don't know the extent
- c) I am fully aware of it and what it implies

18. Meeting online people offline (Children tend to meet in person with the people they met online which might be risky.)

- a) I have never heard about this before
- b) I have heard of it, but I don't know the extent
- c) I am fully aware of it and what it implies

19. The use of acronyms, slang, and codes (Children often used acronyms, slang language, codes to hide their conversation to their guardian).

- a) I have never heard about this before
- b) I have heard of it, but I don't know the meaning of these
- c) I am fully aware of them and know what they mean

20. Internet addiction (Teenagers can spend on average 9 hours online sacrificing other important activities especially time they need to sleep, study).

- a) I have never heard about this before
- b) I have heard of it, but I don't often check
- c) I am fully aware of it and what it implies

21. Rank the terms given below that could pose a real danger to your children online

Treats	Seriousness		
	Very serious	Kind of serious	Not serious at all
Cyberbullying			
Internet addiction			
Acronyms uses			
Meeting online people offline			
Sharing personal information			
Predators			
Identity theft			
Location Sharing			
Predators			
Access to inappropriate content			
Viruses- malware			
Online scams			

Section 3:

This section will try to establish your preference or need regarding information shared in a guide for creating cyber safety awareness and response. It will also help assessing the impact such material would have.

- 22. Who should be involved in cyber safety awareness initiatives for children? Please select who and rate by importance (1 being the most important actor.)
 - a) Government
 - b) Schools
 - c) Teachers
 - d) Parents

- 23. Have you been given material from school about what you should be aware of concerning cyber safety?
 - e) No, we have not
 - f) Yes we have, but I have never read it
 - g) Yes we have, and I know what is inside

- 24. Do you know what are the rules concerning the cyber safety of the school, if there are?
 - a) No, I don't know, and I don't think there are any
 - b) Yes, there are rules, but I don't know them
 - c) Yes, there are rules, and I know them

- 25. Do you need guidance on how to recognize risks and handle them?
 - a) Yes because I don't feel fully prepare/loaded
 - b) I'm not sure
 - c) No, I have enough knowledge

- 26. Do you need guidance on how to communicate about the matter with your child?
 - a) Yes because I don't feel fully prepared/loaded
 - b) I'm not sure
 - c) No, I have enough knowledge

- 27. If yes, in questions 25 and 26 above, how would you prefer the information to be shared? (you may choose more than one option)
 - a. A printed information brochure
 - b. A website with information about cyber safety issues
 - c. An information session at a parent meeting
 - d. Regular information sessions at parent meetings
 - e. An electronic book
 - f. Other? – Please specify?

- 28. What impact do you think would such campaign have on parenting?

-
-
29. What impact do you think would such campaign have on Cyber Safety Awareness?
-
-
-
30. What impact do you think would such campaign have on overall online safety?
-
-
-
31. What would you expect from such an information sharing campaign?
-
-
-
32. What else would you think need to be done in parallel to improve the cyber safety awareness campaign's efficiency?
-
-
-
33. Who has the authority to make this campaign happen?
-
-
-
34. What could restrain the campaign efficiency?
-
-
-

APPENDICES

10.2 APPENDIX B: RESULTS OBTAINED FROM QUESTIONNAIRE

Questions	A	B	C		Questions	A	B	C		Questions	A	B	C	
1	34	14	0		1	70.83	29.17	0.00		1	70.83	29.17	0.00	
2	45	3	0		2	93.75	6.25	0.00		2	93.75	6.25	0.00	
3	23	25	0		3	47.92	52.08	0.00		3	47.92	52.08	0.00	
4	15	20	13		4	31.25	41.67	27.08		4	31.25	41.67	27.08	
7	10	23	15		7	20.83	47.92	31.25		7	20.83	47.92	31.25	
8	4	22	22		8	8.33	45.83	45.83		8	8.33	45.83	45.83	
9	36	10	2		9	75.00	20.83	4.17		9	75.00	20.83	4.17	
10	6	18	24		10	12.50	37.50	50.00		10	12.50	37.50	50.00	
11	4	7	37		11	8.33	14.58	77.08		11	8.33	14.58	77.08	
12	1	13	34		12	2.08	27.08	70.83		12	2.08	27.08	70.83	
13	1	7	40		13	2.08	14.58	83.33		13	2.08	14.58	83.33	
14	3	9	36		14	6.25	18.75	75.00		14	6.25	18.75	75.00	
15	2	9	37		15	4.17	18.75	77.08		15	4.17	18.75	77.08	
16	9	4	35		16	18.75	8.33	72.92		16	18.75	8.33	72.92	
17	3	7	38		17	6.25	14.58	79.17		17	6.25	14.58	79.17	
18	3	8	37		18	6.25	16.67	77.08		18	6.25	16.67	77.08	
19	4	11	33		19	8.33	22.92	68.75		19	8.33	22.92	68.75	
20	1	10	37		20	2.08	20.83	77.08		20	2.08	20.83	77.08	
22	8	7	2	31	22	16.67	14.58	4.17	64.58	22	16.67	14.58	4.17	64.58
23	43	2	3		23	89.58	4.17	6.25		23	89.58	4.17	6.25	
24	26	14	8		24	54.17	29.17	16.67		24	54.17	29.17	16.67	
25	32	10	6		25	66.67	20.83	12.50		25	66.67	20.83	12.50	
26	33	7	8		26	68.75	14.58	16.67		26	68.75	14.58	16.67	

quest 5	Often	Sometimes	Seldom	Never	I do not know what it is	quest 6	Yes and I have used it before	Yes but I have not used it	No	Treats/ quest 21	Seriousness						
											Very serious	Kind of serious	Not serious at all				
Instant messaging (e.g. WhatsApp, MXit, Skype, BBM)	38	5	3	0	2	Changing privacy setting of mobile devices, websites and apps	10	30	8	Treats/ quest 21							
SMS	30	13	5	0	0	Changing preferences for mobile devices, websites, and apps.	29	20	9	Cyberbullying	37	11	0	77.08	22.92	0.00	
Web camera	26	10	4	6	2	Blocking unwelcome adverts, popup messages	20	20	8	Internet addiction	18	30	0	37.50	62.50	0.00	
Voice notes	14	8	12	9	5	Antivirus software	10	32	6	Acronyms uses	19	29	0	39.58	60.42	0.00	
E-mail	24	5	6	13	0	Deleting website download history?	22	16	10	Meeting online people offline	31	17	0	64.58	35.42	0.00	
Online Banking	19	10	4	1	14	Installing/uninstalling applications	30	8	8	Sharing personal information	35	13	0	72.92	27.08	0.00	
Reading news	30	7	3	8	0					Predators	41	7	0	85.42	14.58	0.00	
Social media (e.g. Facebook, Twitter, YouTube, Instagram)	25	4	5	7	7					Identity theft	38	10	0	79.17	20.83	0.00	
Search Engines (e.g. Google, Yahoo!, Bing!)	32	2	9	0	5					Location Sharing	16	32	0	33.33	66.67	0.00	
Gaming apps (e.g. Candy Crush Saga, Pet Rescue Saga)	7	10	17	3	11					Predators	37	11	0	77.08	22.92	0.00	
										Access to inappropriate content	35	13	0	72.92	27.08	0.00	
										Viruses-malware	39	9	0	81.25	18.75	0.00	
										Online scams	32	16	0	66.67	33.33	0.00	

10.3 APPENDIX C: FINAL VERSION OF THE CSINAI SHARED WITH REPRESENTATIVE



Needs Assessment Instrument

Please cross (X) what applies to you.

Section 1 Digital literacy

The first section will help determine the level of comfort you have with a computer/ mobile device and the internet.

1. Do you own a personal computer?
 - a) Yes
 - b) No

2. Do you own a smartphone/cellphone?
 - a) Yes
 - b) No

3. Do you own a tablet?
 - a) Yes
 - b) No

4. How often do per day you use your mobile device(s) (e.g. tablet, smartphone, personal computer)?
 - a) From 0 to 3 hours
 - b) From 3 to 8 hours
 - c) More than 8 hours

5. If yes from question 1, 2 or 3, you use the following apps/functionalities on your devices:

	Often	Sometimes	Seldom	Never	I do not know what it is
Instant messaging (e.g. WhatsApp, Mxit, Skype, BBM)					
SMS					
Web camera					
Voice notes					
E-mail					
Online Banking					
Reading news					
Social media (e.g. Facebook, Twitter, YouTube, Instagram)					
Search Engines (e.g. Google, Yahoo! Bing!)					
Gaming apps (e.g. Candy Crush Saga, Pet Rescue Saga)					

internet browser preferences (e.g. cookies settings)					
--	--	--	--	--	--

6. You are aware of the following:

	Yes and I have used it before	Yes but I have not used it	No
Changing privacy setting of mobile devices, websites and apps			
Changing preferences for mobile devices, websites, and apps.			
Blocking unwelcome adverts, popup messages			
Antivirus software			
Deleting website/download history?			
Installing/uninstalling applications			
Child lock on mobile devices			
Browsing monitoring software			

7. From what age is your child allowed to possess a mobile device (tablet, smartphone)?

- a) Between 7 years old and 10 years old
- b) Between 10 years old and 14 years old
- c) From 14 years old and older

8. From what age is your child allowed to be on social media and browse the internet on its own?

- a) Between 7 years old and 10 years old
- b) Between 10 years old and 14 years old
- c) From 14 years old and older

9. What is your feeling with your child being online?

- a. I am worried and overwhelmed
- b. I don't have any concern
- c. I don't know what to feel

Section 2: Cyber Safety

In each of the following questions, a concept is defined after which you need to indicate your level of awareness of the concept.

10. **Cyber safety** (the wise and responsible use of the internet and technology devices like tablets, and cellphones to be and remain safe online)
 - a) I have never heard about this before
 - b) I have heard of it, but I am not so familiar with this concept
 - c) I am fully aware of the concept and what it implies

11. **Sexting** (the sending and receiving photos or videos where the individuals are naked or partially naked. It also includes sexually suggestive messages sent through text messages or instant messaging).
 - a) I have never heard about this before
 - b) I have heard of it, but I am not so familiar with this concept
 - c) I am fully aware of the concept and what it implies

12. **Cyber bullying** (the use of the internet and technology devices to harass, discriminate and disclose someone's personal information. It is very common among children and can be very devastating.)
 - a) I have never heard about this before
 - b) I have heard of it, but I am not so familiar with this concept
 - c) I am fully aware of the concept and what it implies

13. **Internet** (through which children can access harmful content like pornography, hate speech or through which your device can be infected with viruses or malware).
 - a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies

14. **Predators** (People, paedophiles who exploit and manipulate children via the internet).
 - a) I have never heard about them before
 - b) I have heard of it, but I don't know how to recognise them
 - c) I am fully aware of it and what it implies

15. **Identify theft** (Personal information like identity, pictures shared online on social media or chat-room can be stolen or misused by individuals online).
 - a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies

16. **Location sharing** (People are often geo-tagging themselves to give parents/friends their location. The location sharing option can often be used by predators/stalkers to monitor them).
 - a) I have never heard about this before

- b) I have heard of it, but I don't know the extent
- c) I am fully aware of it and what it implies

17. Sharing of personal information (People especially children tend to share more than they should online like their address, real name, and habits).

- a) I have never heard about this before
- b) I have heard of it, but I don't know the extent
- c) I am fully aware of it and what it implies

18. Meeting online people offline (Children tend to meet in person with the people they met online which might be risky.)

- a) I have never heard about this before
- b) I have heard of it, but I don't know the extent
- c) I am fully aware of it and what it implies

19. The use of acronyms, slang, and codes (Children often used acronyms, slang language, codes to hide their conversation to their guardian).

- a) I have never heard about this before
- b) I have heard of it, but I don't know the meaning of these
- c) I am fully aware of them and know what they mean

20. Internet addiction (Teenagers can spend on average 9 hours online sacrificing other important activities especially time they need to sleep, study).

- a) I have never heard about this before
- b) I have heard of it, but I don't often check
- c) I am fully aware of it and what it implies

21. Rank the terms given below that could pose a real danger to your children online

Treats	Seriousness		
	Very serious	Kind of serious	Not serious at all
Cyberbullying			
Internet addiction			
Acronyms uses			
Meeting online people offline			
Sharing personal information			
Predators			
Identity theft			
Location Sharing			
Predators			
Access to inappropriate content			
Viruses- malware			
Online scams			

Section 3 Communication's preference

The third section will help determine your preference in communication.

22. Have you been given material from school about what you should be aware of concerning cyber safety?
- a) No, we have not
 - b) Yes we have, but I have never read it
 - c) Yes we have, and I know what is inside
23. Do you know what are the rules and policies concerning the cyber safety of the school, if there are?
- a) No, I don't know, and I don't think there are any
 - b) Yes, there are rules, but I don't know them
 - a) Yes, there are rules, and I know them
24. Do you need guidance on how to recognize risks and handle them?
- a) Yes because I don't feel fully prepare/loaded
 - b) I'm not sure
 - c) No, I have enough knowledge
25. Do you need guidance on how to communicate about the matter with your child?
- a) Yes because I don't feel fully prepared/loaded
 - b) I'm not sure
 - c) No, I have enough knowledge
26. How would you prefer the information to be shared? (you may choose more than one option)
- a) Newsletter
 - b) A website with information about cyber safety issues
 - c) Paper base book, journal
 - d) Hand outs (flyers, leaflets)
 - e) An electronic book
 - f) Interactive content (quizzes, games, activity cards)
 - g) videos
 - h) Other? – Please specify?
-
27. When would you like to receive the awareness sessions
- a) Awareness day
 - b) Workshop
 - c) Parents meeting
 - d) Online sessions/correspondence

28. How often are you willing to participate in such an awareness campaign?

- a) Every two weeks
- b) Monthly
- c) Every trimester

29. Would you be willing to be evaluated frequently to insure awareness improvement?

- a) No, I would not be
- b) I don't know
- c) Yes, I would love that

30. What would you expect from such an information sharing campaign?

31. What else would you think need to be done in parallel to improve the cyber safety awareness campaign's efficiency?

10.4 APPENDIX D: CYBER SAFETY AWARENESS MANUAL



Cyber Safety Awareness Manual for Parents

MANUAL FOR EDU X
ELVIRA PARAISO





This document will assist in using the Cyber Safety Information Framework to perform a cyber safety awareness campaign efficiently. This manual is to be used by the Service Provider, Edu X.

It will detail where all the components fit in the process and how they are used.

Following these steps will ensure an effective cyber safety awareness campaign.

Cyber Safety Awareness Campaign

An effective cyber safety awareness campaign should be performed according to the steps detailed below.

Table 1: Cyber Safety Awareness steps through the framework and system

Step	Component	Subcomponent	APPLICATION
1	Identify the role-players		School Government Teachers Parents Children
2	Choose the targeted audience		PARENTS in our case
3	Consult the overall Body Of Knowledge (internationally & in context) to find out	<ul style="list-style-type: none"> - Trending topics - Overall Cyber Safety requirements (digital literacy, personal skills, preliminary awareness) - Available policies/rules/ laws - Possible medium - Possible support/ reaction procedure (recognition, mitigation, reaction, responsibility skills) 	STORED IN THE DATABASE of the System
4	Identify the audience's current skills		Performed using the Cyber Safety Information Needs Assessment Instrument (CSINA)
5	Compare the audience's skills against overall requirements to isolate their specific needs	<ul style="list-style-type: none"> - Skills needed - Topics needed to be covered - Preferred medium, time 	Done through the analysis of the results of the CSINA
6	Compile material according to previous steps		Categorisation



7	Arrange an actual training session	<ul style="list-style-type: none"> - Venue - Tips to keep the audience's interest during training - Trainer and trainee availability 	Arranged by Edu X
8	Evaluate the impact of the training or the material		Future Research

What the Cyber Safety Information Needs Assessment Instrument is and how to apply it

The Cyber Safety Information Needs Assessment Instrument (CSINAI) was developed to evaluate the parent's initial level of digital literacy and cyber safety awareness. It will also indicate the topics to be covered in the awareness campaign, as well as the depths of the information provided.

The first section covers digital literacy. We asked parents about their familiarity with technology and the internet. The second section covers threats and other cyber safety-related topics. We asked parents how familiar they are with these areas to gain an idea on what to include in the awareness campaign ensuring the relevant factors are correctly covered. The third section will be used to establish the parent's knowledge of rules and policies in place in the school and government, as well as to identify the delivery method of the campaign and most convenient times.

To effectively apply the CSINAI, we need to analyse the most recurring answer patterns in each of the sections. A "High", "Medium" or "Low" code is assigned to each question, depending on how it was answered. Table 2, 3 and 4 below highlight how the codes were assigned to each question from the different sections of the questionnaire.

We will define the value of each answer whether it is high, medium or low to determine the ability of each parent.

The most recurring pattern will then be considered as most likely to apply to the parents targeted by a specific campaign.

First section: Digital Literacy

Table 2: Results equivalent for Section 1

Question number	Response A (Often and sometimes)	B or Seldom	C/ Never or I don't know
1	High	Low	NA
2	High	Low	NA
3	High	Low	NA
4	Low	Medium	High
5	High	Medium	Low
6	High	Medium	Low
7	High	Low	Medium
8	High	Low	Medium
9	High	Low	Medium

Considering the data from Table 2, we may say that whenever "High" is a more repetitive pattern, the parents are digitally literate, whenever it is "Medium" the parents would only know the basics and when "Low", they would know very little. This will indicate the level at which the information can be shared during the campaign.

Second Section: Cyber safety awareness

Table 3 Results equivalent for Section 2

Question number	Response A (Often and sometimes)	B or Seldom	C/ Never or I don't know
10	Low	Medium	High
11	Low	Medium	High
12	Low	Medium	High
13	Low	Medium	High
14	Low	Medium	High
15	Low	Medium	High

16	Low	Medium	High
17	Low	Medium	High
18	Low	Medium	High
19	Low	Medium	High
20	Low	Medium	High
21	High	Medium	Low

From the information provided in Table 3, we may say that whenever "High" is a more repetitive pattern, it indicates that the parents are aware of the possible threat, whenever it is "Medium", the parents would only know the basics and when "Low", they would know very little. Considering each threat will give a more comprehensive idea of which threats to emphasise during the campaign.

Third section: Parents' Communication Preference

Table 4 Results equivalent for Section 3

Question number	Response A (Often and sometimes)	B or Seldom	C/ Never or I don't know
22	Low	Medium	High
23	Low	Medium	High
24	Low	Medium	High
25	Low	Medium	High
26	N/A	N/A	N/A
27	N/A	N/A	N/A
28	Low	Medium	High
29	High	Medium	Low
30	N/A	N/A	N/A
31	N/A	N/A	N/A

Considering the information in Table 4, we may say that whenever "High" is a more repetitive pattern, it indicates that the parents are not willing to be contacted often, whenever it is "Medium" the parents are not sure of what they would prefer and with

"Low" they would be open to being contacted often. We could also determine whether they are aware of the governance policies or not.

From the recurring patterns of Questions 26 and 27, the parents preferred delivery time and method could be determined. Questions 30 and 31 are included to allow parents to raise their opinions on the campaign and make suggestions on what can be added or removed to improve the overall campaign.

This analysis part can be automated further if needed.

Example of Results

From the responses of the research sample used for the study, the following results were generated.

Table 3 Results from the research sample

Framework Components	Results	Topics/Items to be included in categorisation
Governance	Low	Provide clear policies from the government and school
Digital Literacy Level	Medium	Give monitoring and security software; teach about hacking, spam, phishing and spoofing
Cyber safety level	Med-high	Regular updates on the most relevant, recurring threats in RSA among the youth Regular updates on slang and new criminals' behaviour
Delivery Method	Most parents prefer information via a printed brochure, 54%, 29% prefer online information	Compile brochure Compile categorisation of useful online content
Delivery Time	Most parents prefer information via a printed	Sent online or given to children to take home

	brochure, 54%, 29% prefer online information	
--	---	--

Application (Interface and Database)

We would assume that a database of potential cyber safety material would have been created beforehand, using the attributes below. The underlying data model of this system is given below. The following tables are included:

- **School:** where all relevant information regarding the school is stored
- **Themes:** where all the themes are stored
- **Topics**
- **Sub-topics**
- **Age group** (with age groups 5 -10, 10 – 12, 12 – 15, 15 -18)
- **Cyber safety awareness levels:** where the levels Low, Medium and High are stored. Each of these levels is determined according to the CSINAI.
- **Digital literacy levels:** where the levels Low, Medium and High are stored. Each of these levels is determined according to the CSINAI.
- **Presentation type:** where the different kinds of presentation are stored. These include a link, pdf, interactive content (games, activity cards), video and workbooks.
- **Content:** where the different links are stored.

To create the categorisation automatically, the Edu X user will have to fill out the Awareness Form below. This categorisation will serve as a base to compile the information shared during a session or to be given as is with the references to the relevant material.

Cyber Safety Awareness Form

1. Please Enter the Relevant Client's Information Needed Below:

School Name:

Location:

Phone Number:

E-mail:

2. Please Rate the Parents' Cyber Safety Awareness Level:

Low
 Medium
 High

3. Please Rate the Parents' Digital Literacy Level:

Low
 Medium
 High

4. Please Select the Age Group of their Children:

5-10
 10-12
 12-15
 15-18

5. Please Select the Relevant Topics to be Included in the Categorisation, you may select more than 1:

Technology Related
 Content Related
 Harassment Related
 Risk of Disclosing Personal Info

6. Please Select the Preferred Type of Resources, you may select more than 1:

Hardcopy Books
 Electronic Document
 Website
 Interactive Content

7. Would you like to Include the School's Policies to the Categorisation?

Yes
 No

Figure 1 Cyber Safety Awareness Form

Using the form above, the user will enter the information collected via the CSINAI.

The form should be filled out as explained below.

1. Enter the information of the school you will be proposing your services to.

APPENDICES



	Security Engagement with children	Security Engagement with children					
Policies		School policies National policies					

The information comprised in the categorisation will be used to compile the materials (brochures, links etc.) that will be shared during the cyber safety awareness campaign training.

Table 7 below shows an example of the populated categorisation, to be used, to possess the relevant information during training.

APPENDICES

Themes	Topic	Subtopics	Digital literacy level	Cyber Safety awareness level	Presentation type	Age group	Link
Cyber Safety threats	Technology related threats	Hacking	med	med	online content	high school children	http://www.waxedmedia.co.za/digitaljungle/hacker_protection_and_cyber_crime_in_south_africa http://cybercrime.org.za/hacking/
		Malware	med	med	online content	high school children	http://sacfis.co.za/viruses.htm http://icode.org.za/home-why.php
		Spyware	med	med	online content	high school children	http://cybercrime.org.za/spyware/
	Content related threats	Exposure to illicit or inappropriate content	low-med	med	online content	high school children	https://saferinternetsouthafrica.co.za/prev-ent-downloading-malicious-app/ https://saferinternetsouthafrica.co.za/selfie-s-nudes/ https://saferinternetsouthafrica.co.za/inapropriate-websites/
	Harassment related threats	Cyber-bullying	med	med	online content	high school children	http://www.cyberbullying.org.za/cyberbullying-in-sa.html http://www.cyberbullying.org.za/uploads/2/7/8/4/27845461/online_abuse_-_adults.pdf https://saferinternetsouthafrica.co.za/topics/cyber-bullying/
		Cyber-stalking	med	med	online content	high school children	http://cybercrime.org.za/cyberstalking/ https://saferinternetsouthafrica.co.za/online-stalking/
Sexting		med	med	online content	high school children	http://www.cyberbullying.org.za/sexting.html https://saferinternetsouthafrica.co.za/sexting/	

APPENDICES

		Predators	low	low	online content	high school children	http://www.cyberbullying.org.za/online-enticement.html http://sacfis.co.za/idtheft.htm http://www.cyberbullying.org.za/child-pornography.html https://saferinternetsouthafrica.co.za/grooming/ https://saferinternetsouthafrica.co.za/online-strangers/
		Scam	low	med	online content	high school children	https://scambuster.co.za/ http://sacfis.co.za/sms.htm http://crimeweb.co.za/
	Risk of exposing information	Phishing	low	low	online content	high school children	https://www.youtube.com/watch?v=0XZzcorg2k4 https://saferinternetsouthafrica.co.za/phishing/
		Social networks/social media	low	low	online content	high school children	http://www.cyberbullying.org.za/being-safe-on-facebook.html http://www.cyberbullying.org.za/being-safe-on-twitter.html http://www.cyberbullying.org.za/being-safe-on-instagram.html http://www.cyberbullying.org.za/im-chat-rooms-and-email.html https://saferinternetsouthafrica.co.za/parents-guide-snapchat-keeping-kids-safe/ https://saferinternetsouthafrica.co.za/topics/social-media-guides/ https://saferinternetsouthafrica.co.za/online-dating/ https://saferinternetsouthafrica.co.za/online-chat/ https://saferinternetsouthafrica.co.za/social-media-networks/ http://www.cyberbullying.org.za/videos.html

APPENDICES



							https://saferinternetsouthafrica.co.za/inappropriate-photographs/
Trends (newest trends)	Slang	Slang	low	low	online content	high school children	http://www.mirror.co.uk/news/uk-news/alarmed-secret-sexing-trolling-codes-9583904
		tips	low	low		high school children	https://saferinternetsouthafrica.co.za/topics/safe-resources/ https://www.facebook.com/staysafeonlineouthafrica https://alertafrica.com/awareness/ https://saferinternetsouthafrica.co.za/prevent-downloading-malicious-app/
Tools	Monitoring	Monitoring	med-high	med-high	software/application	high school children	https://www.kaspersky.co.za/safe-kids https://www.virtuenet.co.za/
	Security	Security	med-high	med-high	software/application	high school children	https://www.kaspersky.co.za/free-antivirus
	Engagement with children	Engagement with children	low	low	online content	high school children	http://sacfis.co.za/safetytips.htm http://www.cyberbullying.org.za/uploads/2/7/8/4/27845461/connected_dot_com_tip_sheet.pdf https://saferinternetsouthafrica.co.za/topics/parental-advice/
Policies		School policies	low	low	online content	high school children	to be provided by School X
		National policies	low	low	pdf	high school children	https://www.gov.za/sites/default/files/39475_gon609.pdf https://www.education.gov.za/Programmes/SafetyinSchools.aspx

APPENDICES



Table 7 Example of Populated Categorisation

10.5 APPENDIX E: REVISED VERSIONS OF CSINAI AND CYBER SAFETY AWARENESS FORM SHARED TO PUBLIC

10.5.1 Layout + Code of the Cyber Safety Awareness Form

```
<!DOCTYPE html>
```

```
<html>
```

```
<body>
```

```
<form action="/action_page.php">
```

```
<h1>Cyber Safety Awareness Form</h1>
```

```
<br>
```

```
<p> <b> 1. Please Enter the Relevant Client's Information Needed Below:</b> </p>
```

School Name:

```
<input type="text" name="name"><br><br>
```

Location:

```
<input type="text" name="location"><br> <br>
```

Phone Number:

```
<input type="text" name="phone" > <br><br>
```

E-mail:

```
<input type="email" name="email">
```

```
<br>
```

```
<p> <b> 2. Please Rate the Parents' Cyber Safety Awareness Level: </b> </p>
```

```
<input type="radio" name="level1" value="low" > Low<br>
```

```
<input type="radio" name="level2" value="med"> Medium<br>
```

```
<input type="radio" name="level3" value="high"> High<br>
```

```
<p> <b> 3. Please Rate the Parents' Digital Literacy Level: </b> </p>
```

```
<input type="radio" name="level1" value="10-12" > Low<br>
```

```
<input type="radio" name="level2" value="12-15"> Medium<br>
```

```
<input type="radio" name="level3" value="15-18"> High<br>
```

```
<p> <b>4. Please Select the Age Group of their Children: </b> </p>
```

APPENDICES

```
<input type="radio" name="age0" value="5-10" > 5-10<br>
<input type="radio" name="age1" value="10-12" > 10-12<br>
  <input type="radio" name="age2" value="12-15"> 12-15<br>
  <input type="radio" name="age3" value="15-18"> 15-18<br>
```

<p> 5. Please Select the Relevant Topics to be Included in the Categorisation, you may select more than 1: </p>

```
<select name="topics" multiple>
  <option value="techno">Technology Related</option>
  <option value="content">Content Related</option>
  <option value="harass">Harassment Related</option>
  <option value="risks"> Risk of Exposing Personal Info</option>
  <option value="Slang"> Acronyms</option>
  <option value="Tools"> Useful Tools</option>
  <option value="Policies">Government & School Policies</option>
</select>
```


<p> 6. Please Select the Preferred Type of Resources, you may select more than 1: </p>

```
<select name="resource" multiple>
  <option value="Book">Hardcopy Books</option>
  <option value="Pdf">Electronic Document</option>
  <option value="website"> Website</option>
  <option value="interactivec"> Interactive Content</option>
  <option value="vid"> Video</option>
</select>
```

<p> 7. Would you like to Include the School's Policies to the Categorisation? </P>

```
<input type="radio" name="Yes" value="yes" > Yes<br>
<input type="radio" name="No" value="no"> No<br><br><br>
```

```
<input type="submit" value= "Compile Report/Categorisation">
</form>
```

</body>

</html>

Cyber Safety Awareness Form

1. Please Enter the Relevant Client's Information Needed Below:

School Name:

Location:

Phone Number:

E-mail:

2. Please Rate the Parents' Cyber Safety Awareness Level:

- Low
- Medium
- High

3. Please Rate the Parents' Digital Literacy Level:

- Low
- Medium
- High

4. Please Select the Age Group of their Children:

- 5-10
- 10-12
- 12-15
- 15-18

5. Please Select the Relevant Topics to be Included in the Categorisation, you may select more than 1:

Technology Related	^
Content Related	
Harassment Related	
Risk of Exposing Personal Info	v

6. Please Select the Preferred Type of Resources, you may select more than 1:

Hardcopy Books	^
Electronic Document	
Website	
Interactive Content	v

7. Would you like to Include the School's Policies to the Categorisation?

- Yes
- No

10.5.2 Final CSINAI



Cyber Safety Information Needs Assessment Instrument

Please mark with an (X) which answer best applies to you.

Section 1: Digital Literacy

This first section will help determine the level of comfort you have with a computer/mobile device and the internet.

1. Do you own a personal computer?
 - a) Yes
 - b) No

2. Do you own a smartphone/cell phone?
 - a) Yes
 - b) No

3. Do you own a tablet?
 - a) Yes
 - b) No

4. What is the duration of your mobile device usage per day, e.g. tablet, smartphone, personal computer?
 - a) 0 to 3 hours
 - b) 3 to 8 hours
 - c) More than 8 hours

5. What is your child's age group?
 - a) 5-10
 - b) 10-12
 - c) 12-15
 - d) 15-18

6. If you answered yes to questions 1, 2 or 3, please rate your usage of the following applications and devices.

	Often	Sometimes	Seldom	Never	I do not know what it is
Instant messaging (e.g. WhatsApp, MXit, Skype, BBM)					
SMS					

Web camera					
Voice notes					
E-mail					
Online Banking					
Reading news					
Social media (e.g. Facebook, Twitter, YouTube, Instagram)					
Search Engines (e.g. Google, Yahoo! Bing!)					
Gaming apps (e.g. Candy Crush Saga, Pet Rescue Saga)					
Internet browser preferences (e.g. cookies settings)					

7. Please rate your familiarity with the following actions:

	Yes and I have used it before	Heard of it but never used/done	No
Changing the privacy setting of mobile devices, websites and apps			
Changing preferences for mobile devices, websites, and apps.			
Blocking unwelcome adverts, popup messages			
Antivirus software			
Deleting website or download history?			
Installing/uninstalling applications			
Child lock on mobile devices			
Browsing monitoring software			

8. At what age would you allow your child to possess a mobile device (tablet, smartphone)?

- a) Between 7 years old and 10 years old
- b) Between 10 years old and 14 years old
- c) From 14 years old and older

9. When is your child allowed to have his/her own social media account or browse the internet on their own?
- a) Between 7 years old and 10 years old
 - b) Between 10 years old and 14 years old
 - c) From 14 years old and older
10. What are your feelings with regards to your child using the internet?
- a. I am worried and overwhelmed
 - b. I don't have any concern
 - c. I don't know what to feel

Section 2: Cyber Safety

In each of the following questions, a concept is defined after which you need to indicate your level of awareness regarding the concept.

11. **Cyber safety:** *The wise and responsible use of the internet and technological devices such as tablets and cell phones to be, and remain, safe online.*
- a) I have never heard about this before
 - b) I have heard of it, but I am not very familiar with this concept
 - c) I am fully aware of the concept and what it implies
12. **Sexting:** *The sending and receiving of photos or videos where the individual/s are partially or fully naked. This also includes sexually suggestive messages transmitted through text messages or instant messaging.*
- a) I have never heard about this before
 - b) I have heard of it, but I am not very familiar with this concept
 - c) I am fully aware of the concept and what it implies
13. **Cyberbullying:** *The use of the internet and technology devices to harass, discriminate and/or disclose someone's personal information. It is very common among children and can be very harmful.*
- a) I have never heard about this before
 - b) I have heard of it, but I am not very familiar with this concept
 - c) I am fully aware of the concept and what it implies
14. **Internet:** *The platform through which children can access harmful content like pornography or hate speech, or through which your device can be infected with viruses or malware.*
- a) I have never heard about this before

- b) I have heard of it, but I was not aware of the impact it could have
 - c) I am fully aware of it and what it implies
15. **Predators:** *People, known as paedophiles, who exploit and manipulate children via the internet.*
- a) I have never heard about them before
 - b) I have heard of them, but I do not know how to recognise them
 - c) I am fully aware of it and what it implies
16. **Identify theft:** *When someone's personal information, like their pictures, address and identity number, are shared online on social media or chat-room platforms and are misused by individuals online.*
- a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies
17. **Location sharing:** *People geo-tagging themselves to give parents/friends their location. The location sharing option can commonly be used by predators/stalkers to monitor them.*
- a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies
18. **Sharing of personal information:** *People, especially children, tend to share more than they should online like their address, real name, and habits.*
- a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies
19. **Meeting online people offline:** *The change from conversing online with someone to meeting them in real life. This is a high-risk situation as it is easy for predators to pose as someone "safe" online.*
- a) I have never heard about this before
 - b) I have heard of it, but I don't know the extent
 - c) I am fully aware of it and what it implies
20. **The use of acronyms, slang and codes:** *The use of acronyms, slang language and/or codes by children to hide their conversation from their parent/guardian.*
- a) I have never heard about this before
 - b) I have heard of it, but I do not know the meaning of these terms
 - c) I am fully aware of them and know what they mean



21. **Internet addiction:** *The overuse of online platforms. Teenagers can spend on average 9 hours online, sacrificing time that should be spent on essential activities such as sleep and studying.*

- a) I have never heard about this before
- b) I have heard of it, but I do not check the amount of time spent online
- c) I am fully aware of it and what it implies

22. Rank the threats given below in terms of the seriousness they pose to your children online

Treats	Seriousness		
	Very serious	Mild	Not serious at all
Cyberbullying			
Internet addiction			
Acronyms use			
Meeting online people offline			
Sharing personal information			
Predators			
Identity theft			
Location Sharing			
Predators			
Access to inappropriate content			
Viruses- malware			
Online scams			

Section 3: Communication Preference

The third section will help determine your choice of communication medium and time.

23. Have you been given material from your child's school regarding what you should be aware of concerning cyber safety?

- a) No, we have not
- b) Yes, we have, but have never read it
- c) Yes, and we have read it extensively

24. If any, do you know the rules and policies concerning the cyber safety of the school?

- a) No, I don't know and I don't think there are any
- b) Yes, there are rules, but I don't know them
- a) Yes, there are rules and I know them

25. Do you need guidance on how to recognise risks and handle them?
- a) Yes, I do not feel prepared/educated enough on the topic
 - b) I am not sure
 - c) No, I have enough knowledge
26. Do you need guidance on how to communicate about the matter with your child?
- a) Yes, I do not feel I know enough to educate my kids on it correctly
 - b) I'm not sure
 - c) No, I have enough knowledge
27. How would you prefer the information to be shared? (You may choose more than one option).
- a) Newsletter
 - b) A website with information about cyber safety issues
 - c) Paper based book, journal
 - d) Handouts (flyers, leaflets)
 - e) An electronic book
 - f) Interactive content (quizzes, games, activity cards)
 - g) Videos
 - h) Other – please specify.
-
28. When would you like to receive the awareness materials?
- a) An awareness day
 - b) Workshop
 - c) Parents meeting
 - d) Online sessions/correspondence
29. How often would you willing to participate in such an awareness campaign?
- a) Every two weeks
 - b) Monthly
 - c) Every three months
30. Would you be willing to be evaluated on a frequent basis to ensure awareness improvement?
- a) No, I would not be
 - b) I don't know
 - c) Yes, I would love that

31. What would you expect from such an information sharing campaign?

32. What else do you think needs to be done in parallel with the campaign, to improve its efficiency?
