An e-Safety Educational Framework in South Africa

Mariska de Lange[1,2] and Rossouw von Solms[2]
Telkom SA Ltd.[1], Private Bag X74, Pretoria 0001
Tel: +27 12 3111034, Fax: +27 12 3234269
and School of ICT
Nelson Mandela Metropolitan University[2]
P. O. Box 77000, Port Elizabeth 6031
Tel: +27 41 504 3604, Fax: +27 41 504 9604

email: mariska.delange@telkom.co.za[1,2]; rossouw.vonsolms@nmmu.ac.za[2]

Abstract – Information and Communication Technology (ICT) has become an integral part of most individuals' lives. The Internet, in particular, may offer numerous opportunities, but individuals should also be aware of the associated risks. Young children are especially vulnerable to online dangers. They utilize Internet technologies from an early age, and should know how to keep themselves and others safe. However, most do not have the required knowledge and expertise to protect themselves. Parents mostly do not understand their children's online behaviour, and are unable to teach their children how to access the web safely and responsibly. A school is the perfect place to teach children safe online behaviour. However, there is currently a lack of e-Safety education in South African schools. The objective of this paper is to propose a framework that might contribute towards the development of an e-Safety culture. The focus is primarily on learners from primary and secondary schools.

Index Terms – cyber security, e-Safety, framework, awareness, education, culture, schools

I. INTRODUCTION

Electronic communication forms part of just about every facet of a modern individual's life [1]. Even the national economy is totally dependent on cyber space today.

On Thursday, 8 March 2012, the cabinet approved a national cyber security policy framework for South Africa. According to the minister of the Presidency, Mr Collins Chabane, the policy aims to "combat cyber warfare, cyber crime and cyber ills", as well as building confidence and trust in the secure use of information and communication technologies [2]. Although this policy framework is currently not publicly available, the draft made it clear that cyber security education and awareness would play a key role in cultivating a cyber security culture among the citizens of South Africa.

The objective of this paper is to propose a framework that exposes South African school learners to cyber security, or e-safety, in an orderly, well-governed manner.

The paper is structured as follows: Section II presents background information regarding cyber security in South Africa. Section III describes the research methodology followed. Section IV introduces an e-Safety framework on how to raise e-Safety awareness and education in South African schools. Section V explains how the e-Safety framework might lead to the cultivation of an e-Safety culture in South Africa. Section VI concludes the paper.

II. CYBER SECURITY IN SOUTH AFRICA

ICT plays an integral role in our lives. Although evolved ICT brings with it a number of opportunities, it also exposes individuals, particularly children, to risks. Children are often unaware of the dangers lurking on the Internet. This leads to unsafe online behaviour, such as posting personal information on public websites. They may also be involved with cyber bullying, and inappropriate, or illegal behaviour. Therefore, the online safety of children is definitely a concern. Children should be made aware of ICT threats from a very young age, in order to keep themselves safe whilst online. On the other hand, many parents are ill-prepared and unaware of these threats, as they do not have the necessary experience, education and expertise themselves. In addition, they may be unaware of the online activities in which their children are involved [3]. Thus, it is clear that a definite generational divide exists between children and their parents as far as cyber activities are concerned.

Consequently, the focus has moved to e-Safety in South African schools. Current national curricula and policies were studied; and it was clearly established that nothing or very little is formally being addressed or implemented as yet. The Department of Basic Education (DBE) has drawn up a few guidelines on e-Safety; however, these cannot guarantee that e-Safety awareness and education will be integrated into the school curricula. Furthermore, teachers may also lack the necessary education and expertise to teach children about e-Safety.

Nevertheless, according to the literature review conducted for this paper, the implementation of e-Safety should be considered essential in the lives of children. This problem is not unique to South Africa; and it exists in most countries. However, in response, a number of countries are establishing e-Safety programmes and implementing these in their school curricula. A number of valuable e-Safety websites were developed, and ambassadors to e-Safety appointed, to help children in need. South Africa is lagging

behind in this regard, and should follow suit. Addressing this shortcoming would contribute to cultivating an e-Safety culture among learners, and subsequently the general population.

III. METHODOLOGY

This research started with a literature review to gather data and to form a theoretical base. Existing conference papers, journals, articles, books, online sources, dissertations, theses, educational and governmental documents were examined. Following this, a survey consisting of interviews and questionnaires was conducted with six school principals from primary and secondary schools in the Nelson Mandela Bay area. The aim was to ascertain whether South African schools have e-Safety topics or related policies built into their curricula. Questionnaires were completed by 1594 primary and secondary school learners to identify online behaviour, opinions and experiences. Additionally, a case study was conducted in the United Kingdom (UK). It consisted of open-ended, informal and conversational interviews with two e-Safety experts, to identify the current status of e-Safety awareness and education in UK schools, and how these are being implemented. Additionally, the interviews highlighted whether the UK faces the same e-Safety issues as South Africa, and whether intervention regarding e-Safety in schools is required.

The Design Science methodology was chosen as the primary research strategy, as the research contribution is in the form of an artifact, specifically in this case, a framework. The Design Science guidelines of Hevner, March, Park and Ram [4] were followed during the development of the proposed framework. The following summarises the seven guidelines of Hevner et al. [4], as followed in this research.

i. Design as an Artifact: In this case, a framework was developed on how to cultivate an e-Safety culture in South African schools by raising awareness and education.

ii. Problem Relevance: The artifact should provide guidance on how to solve a problem. A problem can be defined as the conflict between the current state and the ideal state of a system. Design Science proposes a way to bridge the gap between the current e-Safety state and the ideal e-Safety state in South African schools.

iii. Design Evaluation: Well-executed evaluation methods should be used to evaluate the artifact [5]. The structure of the e-Safety framework was reviewed by two school principals, one from a primary school, and one from a secondary school. The principals were chosen based on their knowledge and expertise of the current e-Safety situation in schools. Informal, conversational interviews were conducted. Their feedback was used to improve the design of the e-Safety framework. Not only has the framework since been reviewed by school principals, but it has also been extensively discussed within peer-reviews and publications. Portions of this research were presented at SACSAW 2011 and ZA-WWW 2011. Based on the feedback from the peer-reviewers and the conference audience, the design of the e-Safety framework was further refined. The case study conducted in the UK also played a contributing role in the refinement of the proposed design.

iv. Research Contributions: This states that the artifact being developed must provide clear contributions. The e-Safety framework serves as the primary contribution of the design process, as it proposes guidelines on how to raise e-Safety awareness and education in South Africa.

v. Research Rigor: This refers to the way in which the research was conducted [4]. Rigorous methods were utilized both in the construction and evaluation of the e-Safety framework. These included an extensive literature review, interviews with school principals, questionnaires with primary and secondary school learners, and a case study in the UK.

vi. Design as a Search Process: This states that when conducting Design Science research, an effective solution to a problem must be found through a thorough search process. This study was conducted over a two-year period, in which different methods and strategies were utilized to develop the e-Safety framework. The work went through various cycles of evaluation and refinement. The fact that the proposed solution was accepted by various audiences would seem to suggest that the proposed solution was the best fit.

vii. Communication of Research: The final guideline states that design research should be communicated to various audiences. As mentioned earlier, portions of this study were presented at SACSAW 2011 and ZA-WWW 2011.

Hevner et al. [4] stated that Design Science research consists of three phases, namely: a thorough investigation of the problem, the construction of an artifact to solve this problem, and an evaluation of the artifact. This research satisfies these criteria.

IV. AN E-SAFETY FRAMEWORK FOR SCHOOLS IN SOUTH AFRICA

This section presents the e-Safety framework that was developed to raise awareness and increase e-Safety education in South African schools. This framework should not be seen as a complete solution to resolve the e-Safety issues in schools, but rather as a means to improve the current situation.

Five fundamental questions were raised prior to the development of the e-Safety framework:

- How can e-Safety be properly integrated into schools?
- Who should be part of the integration process?
- What should be considered important with regard to e-Safety?
- Where can this material be found?
- When can the material be implemented as important e-Safety messages?

These questions were answered using the results and findings from the data collected and the design strategies

followed throughout this research study. The arguments, deductions and conclusions, which were found, led to the identification of a set of underlying criteria, which form the core of the envisaged e-Safety framework:

- Proper governance must be in place;
- The relevant role players must be identified;
- Effective e-Safety topics must be identified;
- Resources using this content should be identified; and
- It must be clear when and where the e-Safety messages must be delivered.

A high-level graphical illustration of the e-Safety framework is presented in Figure 1. The remainder of this section discusses each criterion in more detail.

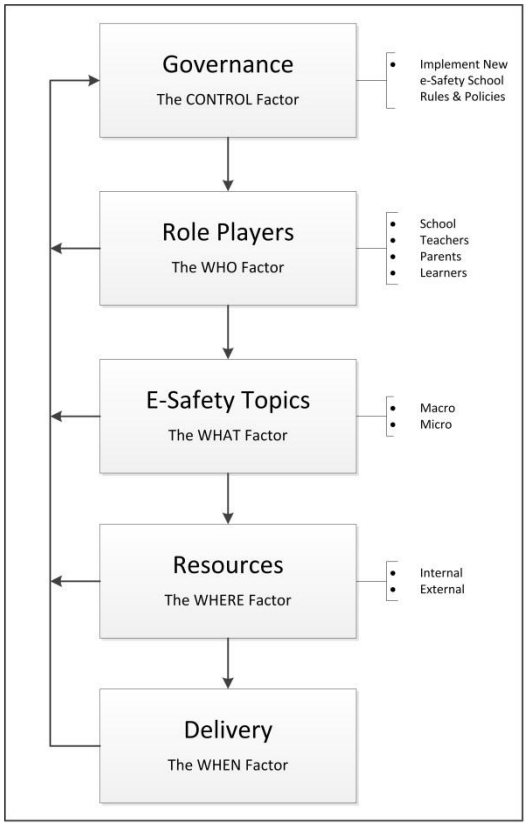

Figure 1: High-level e-Safety framework

A. Governance: The CONTROL Factor

Although ICT provides numerous opportunities, individuals should be aware of the associated risks. Children must be taught how to manage these risks. Educating them in this regard gives children the opportunity to develop safe and responsible online behaviour, whenever they are accessing the Internet. It was unfortunately found that South African schools do not have any form of e-Safety that has been formally implemented. The DBE identified that e-Safety is important; but it has done little to address this issue effectively. They drafted guidelines on e-Safety; however, nothing more has been officially released and implemented in schools yet. These guidelines can only be seen as a minimum requirement. Without implementation, it cannot be guaranteed that this would improve the current e-Safety situation in South African schools. In addition, it was found that there is a lack of e-Safety policies in schools, with no associated school rules. It is clear that governance is a definite problem and must be addressed. It is important that e-Safety policies and school rules must be developed and implemented, so that proper governance is in place. The e-Safety framework focuses on governance by means of the implementation of an e-Safety policy and various school rules.

Becta [6] has stated that implementing an e-Safety policy can help learners to develop safe and responsible online behaviour to keep them safe online. When developing an e-Safety policy, schools must consider covering ICT in its totality. This could be related to fixed technologies provided by the school (ICT in classrooms) or mobile technologies (learners' own mobile phones, laptops, etc.). Therefore, the e-Safety policy must be flexible enough to cover the full scope of ICT relevant to learners, especially with ICT emerging at an immense pace [7]. Descriptions of acceptable and unacceptable uses of ICT may be included in the e-Safety policy, as well as the consequences when the policy gets breached or violated. Supervision and monitoring of the policy should also be discussed. However, the most important component of the e-Safety policy is the defined roles and responsibilities of individuals [6]. For governance to be effective, some role players and definite responsibilities need to be identified – to ensure the effective e-Safety education of children. They must have sufficient knowledge to play their part [7]. Without proper identification of responsibilities, individuals cannot be governed and disciplined properly.

Furthermore, many factors must be considered when developing and implementing an e-Safety policy [7]. These factors will depend on the school itself, namely, the school's infrastructure or its circumstances. In some cases, it must integrate a number of different documents with the e-Safety policy. These documents would be Acceptable Use Policies (AUPs) for learners, parents and staff. An AUP must be clear and concise. It must be consistent with the e-Safety policy, which must be signed by the specific role player who thereby agrees to abide by the rules and statements. Failure to comply with this may lead to disciplinary actions. It is important that all role players who are governed by this policy must understand their specific responsibilities as stated in the policy. Moreover, policies must be reviewed annually to see whether anything regarding e-Safety has changed. The policies should be updated to reflect new changes that have been approved, dated and signed by the governing body.

When talking about e-Safety, children are primarily seen as the most important role players. However, there are other role players involved in the development of safe and responsible online behaviour. These role players will be discussed in more detail in the following sub-section.

B. Role Players: The WHO Factor

Who must be part of the e-Safety integration process? Quite simply: everyone [6]. As mentioned in the previous sub-section, different role players have to be identified for e-Safety governance to be implemented effectively. In addition, these role players have their own unique responsibilities to ensure that e-Safety awareness and

education are raised among learners. Despite this, they must still work together to be effective. The e-Safety policy mentioned in the previous sub-section must apply to all these role players who have access to and are users of ICT, while being at school, or involved with school-related matters. Four different role players were identified:

i. The school (from a governance point of view): For the purpose of this study, the school is sub-divided into three separate role players. This concurs with the governance point-of-view, as they are the role players who have the actual responsibilities and authority on school policies and school rules. These role players can be identified as the governing body, the principal, and the e-Safety coordinator. The governing body may be linked to another 'higher' role player, e.g. the provincial DBE. Therefore, the governing body must take legislation and regulations into account when developing and implementing e-Safety strategies. In order to cultivate an e-Safety culture, the governing body, including the principal, must take on the responsibility and lead the implementation of the e-Safety strategies. Becta also recommends that an e-Safety coordinator be responsible for e-safety in the school. This does not have to be the ICT coordinator; but it could be anyone with the necessary e-Safety knowledge and expertise [6].

ii. The teachers: Teachers may take on four different roles, namely; a learner, advisor, teacher, and an identifier. Becta [6] and Becta [7] argue that the *learner* role does not have enough knowledge and expertise to be able to deliver e-Safety messages to fellow learners. Therefore, teachers must receive training to learn about e-Safety. It is not necessary for them to be experts in the field, but they should know enough to understand the online activities and risks to which learners are exposed. As a result, a teacher may take on the role of a learner. Teachers should also be able to take on the role of *advisor*. Learners may need someone to talk to, and teachers may be seen as trusted parties in whom to confide. Therefore, they must be able to give advice as needed. From the findings of the questionnaire, it was found that teachers are actually the least-trusted parties in this regard, at the moment. Implementing e-Safety in schools would improve this situation. The third role that a teacher may take on, is that of a *teacher* [6]. They must be able to deliver effective e-Safety information in classrooms. Although it was found that e-Safety is not part of the curriculum yet, there may be other areas where it would be appropriate to deliver e-Safety messages to learners [7]. The last teacher role that was identified is that of an *identifier*. Teachers may act as identifiers by noticing changes in a learner's behaviour. These changes may be because of particular e-Safety issues, and the learner may be at risk.

iii. The parents: Parents play an important role in raising e-Safety awareness and education, to help their children develop safe and responsible online behaviour. However, it was found in this research study that some parents do not have the necessary background education and skills to do this. Schools should take the responsibility of involving parents in the process of raising e-Safety awareness and education [6]. In this case, the parents can act as *learners*, because they are being taught about e-Safety. Having acquired a basic level of e-Safety themselves, parents can also take on any of the roles of a learner, advisor, teacher, or an identifier.

After receiving the necessary background education and awareness from the school, the parents should be able to act as *teachers.* Valcke, De Wever, Van Keer and Schellens [8] stated that when parents have more knowledge about ICT and are more active on the Internet themselves, they can then define the rules at home. However, when they have a lack of knowledge and feel they do not have the necessary expertise to access the Internet, they usually prescribe fewer rules for their children. It was also found that younger parents define more rules. This might be because of the generation gap between individuals. Parents must understand that denying children access to the Internet does not solve the problem. The Internet is a resource for education, networking, entertainment, etc. Children must rather be educated on how to be safe online. Parents have the responsibility to ensure that their children receive the necessary e-Safety education, not only at schools, but also at home. Parents may be able to recognize warning signs; therefore, they may act as *identifiers*. Children often know more about ICT than their parents. Thus, it is essential that parents acquire the required knowledge about e-Safety to understand their children's online behaviours. Lastly, parents can act as *advisors*. They must be available when their children need to talk about e-Safety issues. In particular, they must understand and must be able to give the necessary advice to their children.

iv. The learners: The responsibilities of learners should be identified, according to their age, understanding and skill level [6]. Therefore, schools should adopt different responsibilities according to their needs. e-Safety awareness and education must, however, begin at a very young age, in order to try and cultivate an e-Safety culture.

As discussed earlier, teachers and parents may have four different roles. This holds for learners, as well. Learners may have the role of a *teacher* or an *advisor*. It was found that peer-mentoring is very effective among learners. Peer-mentoring occurs when specific learners are trained to encourage other young people to stay safe online; and to show them how to take responsibility for their own actions. Not only can learners teach other young people about e-Safety, but they can teach older individuals about e-Safety, as well. Learners can also offer support to others, thus acting as advisors. It was found that when it comes to e-Safety matters, learners rather than teachers would listen to their friends. Learners may also take on the role of *identifier*, because in most cases learners can recognize when their friends need help. Depending on the seriousness of the e-Safety issue, learners may be able to spot an older individual, and to ask for help. A learner plays the role of a *learner*, when taught about e-Safety issues, and how to stay safe online.

These are, however, not the only role players that can be part of raising e-Safety awareness and education; but they are deemed the most important. Every school must decide what role players are important to them, based on their own school e-Safety environment. However, learners must be seen as the most integral part, when it comes to raising

e-Safety awareness and education, because children are the route towards cultivating an e-Safety culture for the future.

C. Topics: The WHAT Factor

For e-Safety awareness and education to be raised, schools must consider which topics are the most important to focus on, so that these can be linked to the specific role players. e-Safety covers a wide range of topics, and all are considered important.

When talking to the different role players about e-Safety, it is important to discuss the advantages and disadvantages associated with ICT. Individuals must be taught how to handle different e-Safety situations; and they should also develop a risk-awareness skill, to keep themselves safe online. In addition, they must be made aware of the consequences involved. Learners need to be taught where to turn to if they need help with e-Safety issues. The aim of raising e-Safety awareness and education is to change the online behaviour of these individuals. The idea is not to identify and prescribe an extensive list of e-Safety topics, but rather where to locate material to be used in this educational process. This will be discussed in the next sub-section.

D. Resources: The WHERE Factor

Resource locations where e-Safety material can be retrieved are another important aspect of the e-Safety framework. Internal and external resources were identified, which must both be incorporated into the e-Safety framework. Internal resources include any material that is developed by teachers, using their own initiative. This can range from e-Safety videos, activity cards, teachable recipes, presentations to hand-outs [9].

In contrast, external resources consist of material that can be retrieved from existing e-Safety websites. Internal resources may also be retrieved from existing e-Safety websites and be utilized to deliver e-Safety messages to different role players. Various existing websites offer e-Safety material that can be downloaded and utilized free of charge. Some websites offer educational e-Safety games to raise awareness. These resources cover a wide range of different e-Safety topics. A few examples of existing websites are: Thinkuknow (http://www.thinkuknow.co.uk/), KidSmart (http://www.kidsmart.org.uk/), NetSmartzKids (http://www.netsmartzkids.org/) and Kent ICT (http://www.kenttrustweb.org.uk/kentict/kentict_home.cfm).

Internal and external resources must be implemented into the e-Safety awareness and education programmes in schools. Most of these existing websites are designed not to function as a traditional curriculum, but rather as adaptable resources, which can fit anywhere into the existing school curriculum [9]. This creates flexibility. Most of the material can also be tailored, according to ones needs. One issue that needs to be considered is the budget limitation of the school. The e-Safety resources should be chosen with the budget in mind.

In this section, various questions in connection with the proposed e-Safety framework have been answered. However, the question on when it is appropriate to deliver the e-Safety material is still outstanding. This will be answered in the next sub-section.

E. Delivery: The WHEN Factor

From the interviews with principals and the UK case study, it was found that e-Safety messages, aimed at awareness and education among learners, can best be transferred in classrooms. Life Orientation (LO) and Computer Applications Technology (CAT) subjects were chosen to deliver e-Safety material. However, e-Safety awareness and education must be raised among parents, as well. This can be done through awareness days, parent evenings, workshops, leaflets, circular letters and newsletters. In addition, teachers can receive e-Safety training during workshops. These are just a few approaches that can be followed. However, additional approaches can deliver the e-Safety messages to the specific role players. Schools must decide on the best time to deliver e-Safety material. For example, to have a workshop for parents, schools must run workshops at different times, ensuring that more parents are able to attend.

Thus far, governance and the different role players can be seen as the most important components of this proposed e-Safety framework. Understanding their online behaviours and being able to control them, might lead to an e-Safety culture in the future. Therefore, feedback should be given to specific role players. Feedback should be given from the e-Safety coordinator. The final component of the e-Safety framework is to review and refine the e-Safety policies and school rules. All changes should be monitored and reported. e-Safety policies and school rules should be adapted and governed accordingly, in order to strengthen e-Safety governance in the specific school, and to encourage an e-Safety culture. Adopting the guidelines consistently from the e-Safety framework might lead to an e-Safety culture in the future.

V. TOWARDS A CYBER SECURITY CULTURE IN SOUTH AFRICA

The results and findings of the various data collection methods, discussed in Section III, proved that there is a definite lack of e-Safety awareness and education in South Africa. Most people do not understand e-Safety in its entirety. As a result, they are not involved in e-Safety awareness and educational activities. However, it is now known that schools play an important role in educating learners about e-Safety. The aim of the proposed e-Safety framework is to cultivate an e-Safety educational process.

Da Veiga and Eloff [10] stated that the interaction between information security components and the information security behaviour of individuals leads to an information security culture. Similarly, this interaction can be applied to e-Safety. Figure 2 illustrates that e-Safety components (A) can be implemented in the school. These could refer to the proposed e-Safety framework. The e-Safety framework can be seen as the input that influences the e-Safety behaviour of the specific role players (B). The implementation of the e-Safety framework influences the interaction of the role players with certain e-Safety issues within the school. This, in turn, leads to e-Safety behaviour.

e-Safety behaviour then results in safe and responsible use of online activities. In time, when e-Safety changes in the school occur, the e-Safety behaviour of the role players should adapt to the changes. An e-Safety culture (C) would be thereby cultivated.

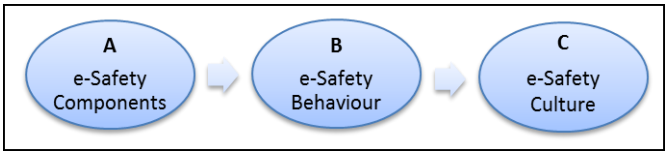

Figure 2: Influencing e-Safety behaviour and cultivating an e-Safety culture (Adapted from [10])

Therefore, implementing the e-Safety framework in schools successfully could contribute to cultivating an e-Safety culture amongst learners at school. This would obviously contribute to the government's aim to establish such a culture amongst all citizens, as spelt out in their national cyber security policy framework.

VI. CONCLUSION

This paper has introduced an e-Safety framework, consisting of guidelines on how to raise e-Safety awareness and education in South African schools. The e-Safety framework has various components that must be considered. Not only is it now known why e-Safety awareness and education are important, but also how to implement these in South African schools. It is imperative that schools draft e-Safety policies and school rules to improve the current situation. Various role players were identified, each with their own responsibilities. These role players are important and must work together, in order to raise e-Safety education and awareness amongst individuals. If the e-Safety framework is properly implemented and managed, it should raise the level of e-Safety awareness, improve the relevant skills, and assist in cultivating an e-Safety culture.

REFERENCES

[1] Wellman, B., & Haythornthwaite, C. A. (2002). The Internet in Everyday Life. New Jersey: Wiley-Blackwell Publishing.

[2] SAPA. (2012, March 8). Cabinet approves cyber security plan. Retrieved May 13, 2012, from News24: http://www.news24.com/SciTech/News/Cabinet-approves-cyber-security-plan-20120308

[3] Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-Safety awareness among young people. Computer Fraud & Security, 13-19.

[4] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 75 - 105.

[5] March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Support Systems, 15, 251 - 266.

[6] Becta. (2009, February). AUPs in context: Establishing safe and responsible online behaviours. Retrieved February 26, 2010, from http://publications.becta.org.uk/display.cfm?resID=39286

[7] Becta. (2005). E-safety: Developing whole-school policies to support effective practice. Retrieved December 1, 2011, from Becta: http://www.becta.org.uk/schools/esafety

[8] Valcke, M., De Wever, B., Van Keer, H., & Schellens, T. (2011). Long-term study of safe Internet use of young children. Computers & Education, 57, 1292 - 1305.

[9] NetSmartz Workshop. (2011). Implementation Guide. Retrieved August 17, 2011, from NetSmartz Workshop: http://www.netsmartz.org/Resources/ImplementationGuide

[10] Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29, 196 - 207.

ACKNOWLEDGEMENTS

The financial assistance of National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.

Mariska de Lange received her Magister Technologiae degree in Information Technology in 2012 from the Nelson Mandela Metropolitan University and is presently working at Telkom SA Ltd. Her research interests include Information Security, Cyber Security, VoIP Security and Vulnerabilities.

Rossouw von Solms holds a PhD-degree from the ex-Rand Afrikaans University. He is the Director of the Institute for ICT Advancement at the NMMU. Rossouw is also currently the immediate past-President of the South African Institute for Computer Scientists and Information Technologists (SAICSIT). He is also a Certified Information Security Manager (CISM).