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

Mvelo Walaza
University of South Africa
South Africa
53315804@mylife.unisa.ac.za

Marianne Loock
University of South Africa
South Africa
loockm@unisa.ac.za

Elmarie Kritzinger
University of South Africa
South Africa
kritze@unisa.ac.za

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

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

1. INTRODUCTION

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

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

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

2. RESEARCH METHODOLOGY

2.1 Background

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

2.2 Problem Statement

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

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

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

2.3. Research questions, objectives and deliverables

The research question as formulated for this study was:

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

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

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

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

2.4. Methodology

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

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

3. LITERATURE REVIEW

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

3.1. ICT Security in South African Education

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

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

3.2. ICT Security Awareness Models and Frameworks in South Africa

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

framework for guiding compliance with information system security policies and regulations in a university.

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

3.3. ICT Security Awareness in South Africa

The usage of ICT across various industries has caused a rise in knowledge economy which is essential for negotiating with the global societies (Gundemeda, 2014). According to Dlamini and Modise (2012) South Africa is one of the top three countries that have been targeted for phishing attacks. This has caused some institutions to embark on initiatives to empower South African citizens. The CEO of the South African Centre for Information Security (SACfIS), Mr. Beza Belayneh, raised a number of concerns when it comes to ICT-related crime in South Africa in the last couple of years. Some of these incidents include the stealing of R50 million worth of airtime from MTN by some East European nationals, a huge amount of money stolen from an Absa account belonging to the CEO of Media24 (Belayneh, 2010).

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

4. BACKGROUND TO THE RESEARCH STUDY

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

Table 10. The gap analysis (Walaza *et al*, 2014)

	A The Information Security Retrieval and Awareness (ISRA) model	**B The Business Model For Information Security**	**C The Comprehensive Information Security Framework (CISF)**	**D The Teacher Development Framework**	**E The Four-In-Balance Model**	**F The Model for ICT Rural Education**
Leadership and governance		X	X		X	
User awareness	X		X			
Information security documentation	X		X			
Policies and standards			X			
Code of best practice			X			
Human factors		X				X
Collaboration and support		X			X	X

ICT training and learning centres			X			X
Measuring and monitoring	X		X			
Innovation and technology		X		X		
Incident management	X		X			
Compliance			X			
School children		X				X

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

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

4.1. An overview of the added components

In the framework that was proposed by Walaza *et al* (2014) it was suggested that certain components had to be introduced to ensure that the proposed framework would be relevant to the South African schooling environment. The components that were added are Language, ICT Security Ombudsman, ICT Security Curriculum, and Information Repositories. The components were added in order to attempt to bridge the gap (identified during the gap analysis) between the two spheres, namely; ICT security and ICT in education. It was also an attempt to make the proposed framework more relevant to South Africa.

4.2. Language

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

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

4.3. ICT Security Ombudsman

The establishment of an ICT security ombudsman office was a notion that was proposed by this research study. The literature review has revealed that such an office does not exist in South Africa. However, since a vast number of ICT-related crimes have occurred in recent years in the country (Belayneh, 2010), such an office would be very beneficial to South Africa. Walaza *et al* (2014) referred to the high crime rate in South Africa and stressed the need for proper ICT security measures to be put in place.

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

4.4. ICT Security Curriculum

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

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

4.5. Information Repositories

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

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

5. THE PROPOSED FRAMEWORK

The proposed framework was named the ICT Security Awareness Framework for Education (ISAFE). This section presented the different phases of the proposed framework.

5.1. The Leadership & Governance component

The Leadership & Governance component was derived from the Comprehensive Information Security Framework (CISF) (Da Veiga, 2008). The South African government will have to play a leadership and governing role when it comes to the integration of ICT security awareness in South Africa's education system.

5.2. The Documentation component

The Documentation component was derived from the ISRA (Kritzinger, 2006) model. This building block will be used for all the documentation that is relevant to ICT security awareness in South

African schools. Within this component are sub-components that depict the ICT security documentation in literature which will be used to ensure the effective integration of the education and security awareness spheres. Figure 1 depicts the components within the Documentation sub-component.

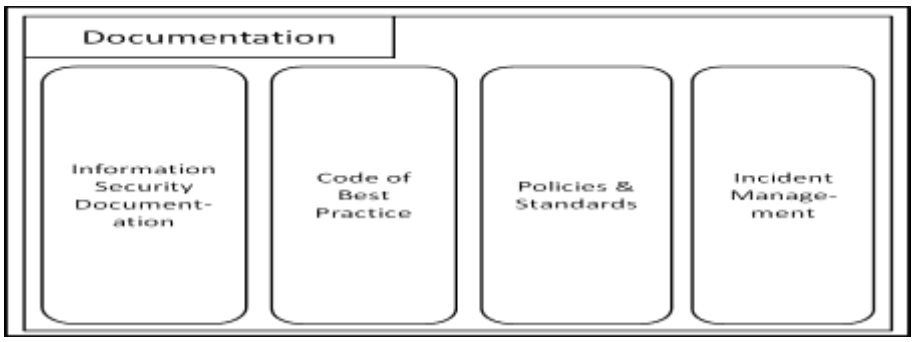

Figure 11: The Documentation component

The sub-components within the Documentation component – Information Security Documentation, Code of Best Practice, Policies & Standards, and Incident Management – were discussed briefly in the paragraphs below.

Information Security Documentation: This sub-component was derived from the ISRA model and it involves all the documentation related to information security. This is the documentation that will be made available to South African school learners in order to enhance their ICT security awareness.

Code of Best Practice: This sub-component was derived from the CISF. This component investigates the code of best of practice for ICT security in South Africa and will encourage school learners to read and adhere to these practices.

Policies and Standards: This sub-component was derived from the CISF and it involves the best policies and standards that must be adhered to by school learners in South Africa. The latter will be encouraged to follow and adhere to the policies and standards that govern the usage of ICT at all times.

Incident Management: This sub-component was taken from the CISF framework. This component will be responsible for the documentation of all incident management procedures that must be followed by school learners.

5.3. The Collaboration & Support component

This component was derived from the Four-In-Balance Model. In the present research study, the collaboration & support component will be accountable for integrating the two spheres (ICT security models and ICT in education models). This component contains a number of sub-components that are used to ensure the integration of ICT security awareness in South African schools. Figure 2 depicts the Collaboration & Support component of the proposed ISAFE.

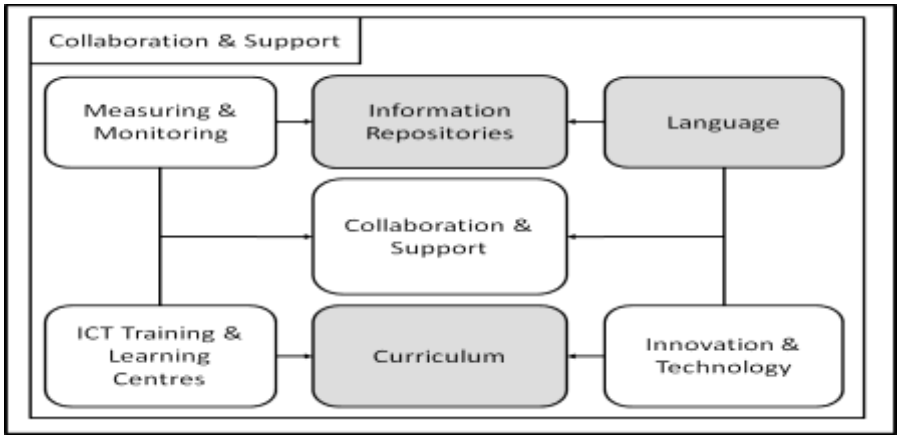

Figure 12: The Collaboration & Support component

The four sub-components of the Collaboration & Support component are Measuring & Support, Collaboration & Support, ICT Training & Learning Centres, and Innovation & Technology. The researcher earlier introduced additional ICT components to make the proposed framework more relevant to South Africa (inter alia Information Repositories, Language, Curriculum) and these were discussed in Section 4.1. The remaining components are discussed in the upcoming paragraphs.

Measuring & Monitoring: This sub-component, which was derived from the ISRA model, is responsible for measuring and monitoring ICT security awareness among school learners in South Africa.
Collaboration & Support: This sub-component was derived from the Four-In-Balance Model. In the present research this component will be used to facilitate collaboration in respect of the dispensing of ICT security information among education institutions in South Africa.
ICT Training & Learning Centres: This sub-component was derived from the Model for ICT Rural Education (Roy, 2012). The current study proposes the establishment of training and learning centres to assist with introducing ICT security awareness among school learners.
Innovation & Technology: This sub-component was derived from both the Teacher Development Framework (Department of Education, 2007) and the Business Model for Information Security (ISACA, 2009). Technology in the form of mobile phones, mobile apps and websites will be utilized to enhance and integrate ICT security awareness in South African schools.

5.4. The People component

This component was derived from the Business Model for Information Security (ISACA, 2009). It is responsible for all the human aspects of this study. The proposed new sub-component, ICT Security Ombudsman, will also be depicted here. The sub-components of the People component of the proposed ISAFE are illustrated in Figure 3 below.

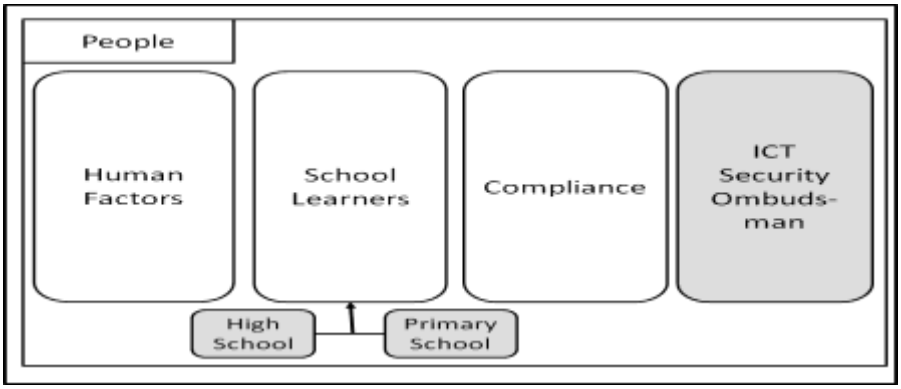

Figure 13: The People Component

The initial sub-components within the People component were Human Factors, School Learners and Compliance. The ICT Security Ombudsman was discussed earlier (in Section 4.1) as one of the new components that were included in the ISAFE. The School Learners component introduces two sub-components called High School and Primary School. These and the rest of the components were discussed in the following paragraphs.

Human Factors. This sub-component was derived from the Business Model for Information Security (ISACA, 2009). This component will investigate some of the human factors that might influence ICT security awareness among South African school learners.

School Learners. The School Learners sub-component, which is one of the main components of the current research study, was derived from the Model for ICT Rural Education (Roy, 2012). The researcher proposed the addition of two sub-components called High School and Primary School to this component, so as to make a distinction between the two types of school learners. Caution must be exercised in respect of the type of information made available to high school and primary school learners.

Compliance. This sub-component was derived from the CISF. It investigates policy compliance among ICT stakeholders in South Africa, specifically among school learners.

5.5. The User Awareness component

The User Awareness component was derived from the CISF. It is responsible for all the ICT security awareness programmes and initiatives that will be directed towards the South African school learners.

6. THE ICT SECURITY AWARENESS FRAMEWORK FOR EDUCATION

The whole ISAFE, showing all the components and their sub-components, was depicted in Figure 4.

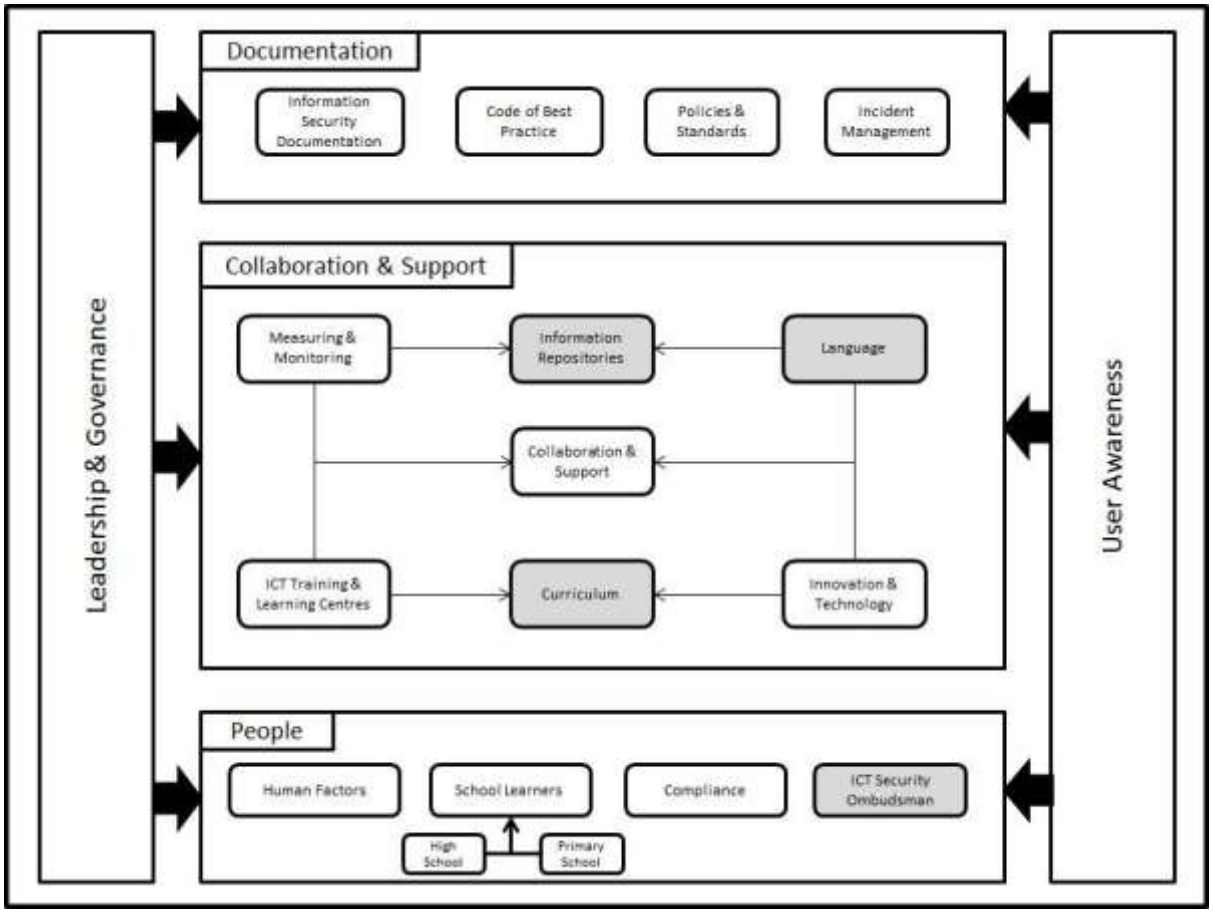

Figure 14: ICT Security Awareness Framework for Education (ISAFE)

The sub-components that have been newly proposed were coloured grey in the framework so as to distinguish them, from those building blocks in Table 1 that were derived from existing models and frameworks.

As indicated earlier, the main purpose of the ISAFE was the integration of ICT security awareness in South African education. The literature review conducted by the researcher indicated that the existing models and frameworks were not adequately relevant to South Africa. Hence a new framework that would be more applicable to South Africa had to be proposed.

7. FINDINGS

A notable gap between ICT security models and frameworks on the one hand and the ICT in education models and frameworks on the other has been discovered. The review revealed that there was a need for an ICT security framework that is relevant to South Africa. A comparison was done by drawing up a gap analysis table showing both the ICT security frameworks and the ICT in education frameworks. The gap that was identified between these two spheres was depicted in Table 1, and hence the researcher proposed an adjusted and more relevant framework for South Africa.

The proposed framework, called the ISAFE, attempted to bridge the gap that was identified in this research study and the researcher was of the belief that it was far more relevant in the South African context. The ISAFE is made up of five main components that were discussed in Section 5. These components were identified as building blocks during the literature review and they contain specific sub-components that were more descriptive. Four new components that were not part of the initial building blocks have been included in this proposed framework and were discussed in Section 4.1.

8. CONCLUSION

This article presented an in-depth discussion of the ISAFE. New components, namely Language, ICT Security Ombudsman, ICT Security Curriculum, and Information Repositories were discussed and were believed to make the proposed framework (ISAFE) more relevant to the South African environment. In Section 2 the researcher explained the research methodology, while the problem statement, the research question, research objectives, and research deliverables were subsequently discussed in separate subsections. In Section 3 the literature review that had been conducted for this research was depicted; and this was followed by the background to the research study in Section 4. The different spheres of the proposed framework were reviewed in Section 5, and this was followed by the proposed framework in Section 6; while the findings of the research were discussed in Section 7.

REFERENCES

Belayneh, B. (2010). South African Centre for Information Security. Retrieved from http://www.sacfis.co.za/index.htm

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

Da Veiga, A. (2008). *Cultivating and Assessing Information Security Culture*. University of Pretoria. Retrieved from https://pdf-source.net/download/2123349/pdf-source-dot-net-repository-up-ac-za.pdf

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

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

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

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

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

ISACA. (2009). An Introduction to the Business Model for Information Security. Retrieved from http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

Kritzinger, E. (2006). *An Information Security Retrieval And Awareness Model For Industry*. University of South Africa. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/2475/thesis.pdf?sequence=1

Kritzinger, E., & Padayachee, K. (2007). Teaching Safe and Secure usage of ICTs in South African Schools. In *Proceedings of the 2nd International Conference on Society and Information Technologies* (pp. 1–6). Pretoria. Retrieved from http://hdl.handle.net/10500/3986

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

MyBroadband. (2014). SA students pour R6.1 billion into tech. Retrieved from http://businesstech.co.za/news/general/55685/sa-students-pour-r6-1-billion-into-tech/

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

Roy, A., Kihoza, P., Sihonen, J., Vesisenaho, M., & Tukiainen, M. (2014). Promoting proper education for sustainability: An exploratory study of ICT enhanced Problem Based Learning in a developing country. *International Journal of Education and Development Using Information and Communication Technology*, *10*(1), 70–90.

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

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

UNESCO. (2012). Why Language Matters for the Millenium Development Goals. In *Language, Education and the Millennium Development Goals*. Bangkok: UNESCO Bangkok. Retrieved from <http://unesdoc.unesco.org/images/0021/002152/215296E.pdf

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

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