# A conceptual framework for cyber-security awareness and education in SA

Noluxolo Kortjan, Rossouw von Solms

School of ICT, Nelson Mandela Metropolitan University, South Africa

## ABSTRACT

The Internet is becoming increasingly interwoven in the daily lives of many individuals, organisations and nations. It has, to a large extent, had a positive effect on the way people communicate. It has also introduced new avenues for business; and it has offered nations an opportunity to govern online. Nevertheless, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks, of which many Internet users are not aware. As such, various countries have developed and implemented cyber-security awareness and education measures to counter the perceived ignorance of the Internet users. However, there is currently a definite lack in South Africa (SA) in this regard; as there are currently, little government-led and sponsored cyber-security awareness and education initiatives. The primary research objective of this paper, therefore, is to propose a cyber-security awareness and education framework for SA that would assist in creating a cyber-secure culture in SA among all of the users of the Internet. This framework will be developed on the basis of key factors extrapolated from a comparative analysis of relevant developed countries.

KEYWORDS: South Africa, cyber-security, cyber-security awareness and education

CATEGORIES: K.4, K.6.5

## 1 INTRODUCTION

> We are currently living in an age where the use of the Internet has become second nature to millions of people. [1]

However, the Internet continues to be threatened by numerous risks, such as that of online crime [2]. Core to criminal activities on the Internet is the exploitation of private information [3]. Thus, Internet users are at risk of having their private information compromised and misused.

According to Thomson, Von Solms and Louw [4], many users lack awareness and knowledge; consequently, they are ignorant of the need to protect their personal and confidential information. Moreover, users' insecure online behaviour makes them easy targets for exploitation. The lack of cyber-security awareness amongst adults negatively impacts their role of protecting the children in their care [5] [6].

De Lange and Von Solms [7] argue that many parents are not knowledgeable of the threats apparent online; and therefore, they are unable to teach their children about secure online behaviour. As such, the safety of children is also compromised.

Lack of knowledge is viewed as an important factor that contributes to insecure online behaviour by Internet users. As a result, people are seen as "a severe threat to each other's security" [8]. In addition, such lack of the relevant knowledge has made the African population easy targets for hackers and botnet operators [9].

In view of the consequences of the lack of knowledge, cyber-security and awareness therefore become issues of fundamental importance. Christensen [10] affirms that promoting cyber-security awareness would contribute greatly towards cyber-security as a whole. Awareness and education can provide Internet users with the ability to recognise and circumvent any risks that are apparent online [11]. Additionally, education plays a critical part in cultivating a culture of secure behaviour amongst Internet users. While the working class may be getting some form of cyber-security awareness and education from industry, for home users and society at large, a national campaign for cyber-security awareness and education is urgently required [10].

In this context, it is the role of the government to empower all levels of society – by providing the necessary knowledge and expertise to act securely online. However, there is currently a definite deficiency in SA in this regard, as there are currently little government-led and sponsored cyber-security awareness and education initiatives [12]. Therefore, the primary research objective addressed in this paper is to propose a cyber-security awareness and education framework for SA that would assist in creating a cyber-secure culture in SA among all of the users of the Internet.

The following section will briefly discuss the current cyber-security efforts in SA.

**Email:** Noluxolo Kortjan Noluxolo.Kortjan@nmmu.ac.za, Rossouw von Solms Rossouw.VonSolms@nmmu.ac.za

## 2 CYBER-SECURITY EFFORTS IN SOUTH AFRICA

AS SA becomes ever more reliant on cyberspace to govern and to conduct business; it is increasingly being exposed to cyber threats [13]. In the year 2010, the South African government released a Draft Cyber-Security Policy [14]. This draft policy implied that SA is not currently in a position to deal effectively with cyber-related threats. Additionally, the draft policy stated that SA lags behind other countries in the development of cyber-security protocols and standards, as well as in the implementation of such protocols and standards.

Articulated in this draft policy framework is the intent to secure cyberspace, and to ensure the protection of SA's national critical information infrastructure. This draft policy framework aims to create a knowledgeable society that understands cyber-related threats. Moreover, it intends to provide a cyber-security approach that is holistic; and, in doing so, it requires the support of all role-players, such as the State, the public and private sectors, and society at large [15].

This draft policy framework is based on the assumption that SA wishes to cultivate a cyber-security culture amongst its citizens and society. As such, cyber-security awareness and education are critical components in such a culture [13]. Conversely, the draft policy framework at hand is silent regarding cyber-security awareness and education. In addition, in 2012 the Department of Communication announced that a cyber-security awareness strategy was being developed. However, such a strategy has not yet been published. Consequently, SA does not yet have a government-initiated cyber-security awareness programme, together with education initiatives, in place [16].

There are, however, currently existing cyber-security awareness and education initiatives in SA. Nelson Mandela Metropolitan University (NMMU) has partnered with the University of Johannesburg (UJ) and the University of South Africa (UNISA) to form a cyber-security awareness campaign. This has been called the South African Cyber-Security Academic Alliance (SACSAA) [17].

The primary objective of SACSAA is to "campaign for the effective delivery of Cyber-Security Awareness throughout South Africa – to all groupings of the population". As the means to reach its objective, SACSAA annually hosts, amongst other initiatives, a National Cyber-Security Awareness Week. In this week, a poster competition to engage primary schools is held [17].

In addition, SACSAA is also part of a community-development project co-ordinated by UNISA. This initiative is named the Cyber-Security Awareness Community-Engagement Project (CSACEP) [18]. The primary objective of this project is to spread cyber-security awareness in SA, primarily amongst school children. Amongst other things, this project makes use of the following resources to reach the people:

- workshops
- seminars
- posters
- banners

The Council for Scientific and Industrial Research (CSIR) also promotes cyber-security awareness and education in SA. The CSIR utilises the month of October, the international cyber-security month, to host a series of cyber-security awareness events [19]. Included in these events are practical cyber-security awareness guidelines on topics, such as mobile phone hacking, cyber terrorism and information warfare. The events held in the cyber-security month may vary annually.

The initiatives above are offered by academic institutions and the science council. Although both of these are government-funded bodies, there are currently no direct government-led or government-sponsored campaigns. The proposed, or similar, framework for cyber-security awareness and education for SA will, if implemented and used by the SA government, contribute to creating the envisaged cyber-secure culture in SA amongst its citizens and users of the Internet. Following is a brief description of the methodology used to articulate the proposed framework.

## 3 THE RESEARCH METHODOLOGY

This paper proposes a cyber-security awareness and education framework, in the form of an artefact. Similarly, design science concerns itself with creating an artefact as a solution to such a problem [20]. Consequently, this research was conducted in the design science-research paradigm.

There are various approaches to design science, one of which is that defined by Peffers and his colleagues [21]. Peffers et al. have developed a design-science approach that is consistent with the design-science processes in other disciplines. This approach provides a method for conducting research. Furthermore, provides a mental model of what the research output should resemble. On the basis of the aforementioned factors, this approach was followed in this research [21].

According to the selected research approach, six definite steps, as listed below, were followed.

**Problem identification and motivation.** Identifying the problem, while motivating the value of a solution.

**Objectives of a solution.** Deducing the objective of the solution from the identified problem.

**Design and development.** Creating a solution in the form of an artefact.

**Demonstration.** Demonstrating the efficacy of the artefact for solving the problem.

**Evaluation.** Observing and measuring how well the artefact supports a solution to the problem.

**Communication.** Creating scholarly and/or professional publications.

These steps are intended to guide the researcher. Therefore, this research has closely followed the declared steps, using the relevant research methods at each step

of the process, in order to produce the expected outcome. The research methods that were employed in this study are as follows:

- literature review
- comparative analyses
- argumentation
- elite/expert interviews

In line with Hofstee [22], a literature review was initially conducted, in order to gain insight and understanding of the research area, as well as to bring clarity and focus to the research problem, as stated in Subsection 1.2. Thereafter, a comparative analysis on selected developed countries was performed. According to Mills, Van de Bunt, and De Bruijn, "the underlying goal of comparative analysis is to search for similarity and variance" [23].

From the similarities and variances of the countries studied, certain key factors pertaining to cyber-security awareness and education were forthcoming.

An initial set of key factors was published and reviewed, using peer reviews; and this set was subsequently presented at the AFRICOMM 2012 conference [24]. Based on the feedback obtained from the conference, these factors were adapted accordingly. Subsequently, the proposed cyber-security awareness and education framework was developed – on the basis of these key factors. This will be discussed further in the following section.

From the research paradigm utilised in this study – design science – evaluation is deemed to be a very important component. Through evaluation, the extent to which the artefact supports the solution to the identified problem situation can be measured [25]. Furthermore, the use of well-executed evaluation methods also demonstrates the quality of an artefact [20].

This makes it possible to address both the demonstration and the evaluation steps of design science. These steps were addressed by using elite/expert interviews as the evaluation procedure. Elite/expert interviews can be defined as "a discussion with someone knowledgeable about a problem, or its possible solution" [26]. Elite/expert interviews are semi-structured interviews. As such, they are flexible in nature, and do not require a standard set of questions, in order to be included in the interview guide. In this form of interview, the interview guide consists of a list of themes, and these themes largely guide the questions asked. However, questions vary from respondent to respondent.

According to Cooper and Schindler [26], this method of interviewing is used to discuss a subject with a knowledgeable person: the 'elite'. Hochschild [27], Marshall and Rosman [28], and Tansey [29] shed light on some of the advantages of elite/expert interviews. These advantages are outlined below.

- The interviewer has the opportunity to triangulate information among interviewees – without revealing the names of any other respondents.
- Elites are more capable of providing a general view of a particular subject.
- The interviewees are able to provide valuable information, as a result of their respective positions.

With elite/expert interviews, the interviewer has the opportunity to probe a topic in depth, in order to gain more insight and understanding on a particular subject. The subject in this case is cyber-security awareness, together with education. Thus, the chosen elites should be knowledgeable on the subjects of cyber-security awareness and education.

Marshall and Rossman [28] define an elite individual as someone who is influential, prominent and well-informed about a particular area in the research study. Hochschild [27] further maintains that the person's position is also a contributing factor when considering elites. There are known categories of elites, namely, ultra-elites and professional elites.

Zuckerman [30] refers to ultra-elites as individuals who possess a lot of power within a group of elite individuals; while McDowell [31] defines professional elites as "highly-skilled, professionally competent and class-specific [individuals]".

Smith [32] argues that researchers define the term 'elite' in a manner that is subjective to the relevant respondents. By contrast, this research will not seek a new definition for the term 'elite'; it will merely adopt the definition provided by Marshall and Rossman [28].

Owing to the nature of elites, gaining access can be a challenge [33]. However, in the case of this research, access was gained comparatively easily. Contrary to Conti and O'Neil [34], who recommend the use of formal letters, followed by phone calls to make contact with elites, emails were used. This decision was influenced by the electronic nature of the modern day. As such, using emails to contact the elites proved to work well, as they provided prompt responses.

In this study, the elites where chosen, based on their line of work, experience and knowledge in the field of cyber-security, and particularly in the domains of cyber-awareness and education. Two elites where selected to review the proposed framework in an elite interview.

Elite one works for the CSIR as a cyber-security Specialist and researcher in a Cyber Defense for Scientific Research Group. Moreover, elite one has published a number of research articles on national cyber-security awareness and education. Elite two is the Research Group Leader of the Cyber Defense for Scientific Research at the CSIR. Elite two has spent more than 20 years in academia. Likewise, elite two has also published a number of journal articles and presented numerous conference papers at national and international conferences on the subject of cyber-security.

As such, the framework was revised accordingly, based on the feedback received from the elites. An account of the verification of this framework is elaborated on in Section 6.

This section has provided a brief overview of the research process followed in this study. Moving forward is a brief elaboration of the comparative analysis, which was performed, and the presentation of the cyber-security awareness and key educational factors.

# 4 CYBER-SECURITY AWARENESS AND KEY EDUCATIONAL FACTORS

To explore the way other countries promote cyber-security awareness and education, a comparative analysis of four developed countries was conducted. This comparative analysis focused on the national cyber-security strategies of these countries, as well as on particular nationally initiated and driven cyber-security awareness and education initiatives. From this analysis, the principal factors will be extrapolated, in order to form the basis of a similar envisaged cyber-security awareness and educational framework for SA.

The countries analysed were: the United States of America (USA), the United Kingdom (UK), Australia, and Canada. These countries were chosen because all of them have national cyber-security strategies; they all have at least one national sponsored cyber-security education and awareness initiative; and they are listed in the Organization for Economic Co-operation and Development (OECD).

Being a member of the OECD is of relevance to the study, because this organization promotes the development of policies that improve a country's economic and social wellbeing [35]. The analysis was based on the following thematic questions:

1. Why are cyber-security awareness and education important to the country?
2. What is the country's foremost aim regarding cyber-security awareness and education?
3. Who is assigned the duty to oversee cyber-security awareness and education-related tasks?
4. How is the country planning to work towards cyber-security awareness and education?
5. When can the implementation of cyber-security awareness and education initiatives be expected?

## 4.1 Why are cyber-security awareness and education important to the country?

In the four countries investigated, it is evident that cyber-security awareness and education efforts are the result of a national directive outlined in the respective national cyber-security policies. From these policies, it can be seen that each country has a particular objective behind the issues of cyber-security awareness and education.

In the US, the primary purpose is deeply rooted in protecting the national critical infrastructure [36]. In the UK, on the other hand, the main reason behind cyber-security awareness and education is to serve as a tool for accomplishing its high-level cyber-security objectives [37]. In Canada and Australia, the growing reliance on cyberspace has greatly influenced the economy of these countries. Thus, strengthening their respective economic stance, cyber-security awareness and education should be included as high-level cyber-security objectives in the national cyber-security policies [38].

It may, therefore, be concluded that the rationale behind pursuing cyber-security awareness and education varies from country to country. Moreover, in all these cases, the national cyber-security awareness and education campaigns are a consequence of the respective national policies. Thus, it can be argued that a country should consider cyber-security awareness and education in its own context, in order to understand how it would benefit therefrom. These issues should be solidly founded in any national policy.

## 4.2 What is the community's foremost aim regarding cyber-security awareness and education?

In the US, the goal of cyber-security awareness and education is to raise the level of awareness in the nation on the risks of cyberspace, and how to circumvent these risks [39]. In the UK, the goal is to support individuals and businesses, by informing and educating them on the issue of cyber-security [37]. Finally, in Australia and Canada, the ultimate goal is a cyber-security culture that could be fostered through awareness and education [38], [40].

From these four countries, one can see that the purpose of promoting cyber-security awareness and education is accompanied by certain goals that have been set. As such, setting definite goals should be regarded as vital, as this sheds light on what the country wants to achieve. Furthermore, it also sets some targets, whereby progress can be measured.

## 4.3 Who is assigned the duty of overseeing cyber-security awareness and education-related tasks?

In the USA, a national organisation, The National Initiative for Cyber-security Education (NICE), has been formed. This is entirely dedicated to cyber-security awareness and education [39]. NICE is constituted from a combination of governmental departments. Some of these departments assume the role of leading certain directives that exist within NICE. In the case of the UK, cyber-security awareness and education have been delegated to an external organisation: Get Safe Online.

Similar to the US, in Australia, multiple governmental departments form the focal point of cyber-security awareness and education. However, in Australia, it was noted that there is no partnership between the departments; and this causes some confusion to the target audience about which source to trust [41]. Finally, in Canada, Public Safety Canada takes the lead in cyber-security awareness and education.

In all these countries, it is evident that the documented cyber-security awareness and education goal is assigned to one or more departments or organisations to carry out. This allocation of responsibilities promotes accountability; and furthermore, it establishes a focal point. Thus, there should be a dedicated administration that could serve as a focal point for cyber-security awareness and the implementation of educational initiatives.

### 4.4 How is the country planning to work towards cyber-security awareness and education?

Following the publication of the national cyber-security policies, the US and Canada published action plans outlining their approach to cyber-security awareness and education [39], [42]. The NICE Strategic Plan indicates that campaigns, such as Stop. Think. Connect, could be used to equip the US' public with the necessary knowledge and skills. As indicated, Stop. Think. Connect is well-designed; and through it, more sub-campaigns and programmes could be made available.

Canada's plan presents the actions to be taken to accomplish each of the objectives that are defined in the national cyber-security policy. In addition, it states the timelines and the status of every deliverable, together with the lead department [42]. This action plan clearly encapsulates the actions to be taken, the timelines, and the current status of progress, together with the lead department.

In contrast to the US and Canada, the UK and Australia have not published any action plans in addition to their national cyber-security strategies. However, in Australia, an inquiry that was performed to determine the position of this country concerning cyber-security awareness and education recommended that an action plan be drafted. Therefore, it may be concluded that there should be a strategy in place that clearly articulates how a country should approach cyber-security awareness and education.

National cyber-security awareness and the educational initiatives of each country were analysed, as part of this inquiry. This was done primarily, because these initiatives are, in fact, a major element of how each country is promoting cyber-security awareness and education. The criteria used in the analysis are listed as follows:

**Host organisation**. The department or organisation that will be leading the initiative.

**Target audience**. The grouping of people that the initiative targets.

**Topics covered**. The topics that are covered by the content of the initiative.

**Campaign tools**. The methods that are to be used to deliver the message.

Having examined some of the national cyber-security awareness and educational initiatives of the relevant countries, a number of deductions were made. Firstly, the focus of the cyber-security awareness and education campaigns and programmes should be on every grouping of society. These groupings should include: parents, children, teachers and employees in businesses. This focus is essential, as individuals, organisations and nations are equally exposed to the risks posed in cyberspace [43] [44] [45] [46] [47] [48] [49].

Secondly, each target audience should be presented with topics that are relevant to them. This suggests that research has to be done to identify the individual awareness and educational needs. This relationship between the target audiences and the topics is apparent in the cases of the business environment and children. For example, knowledge about cyber bullying is directed primarily at individuals, and not at the business environment; similarly knowledge about cyber-security policy making is directed at organisations, and not really at children.

Therefore, it is important for cyber-security awareness and education campaigns and programmes to present each target audience with those topics that are relevant to them.

Thirdly, there is a difference in the medium of communication used to deliver the awareness-raising and education information to a particular audience. Using the same example of organisations and children, it can be seen that from the analysis that children are often presented with cyber-security awareness and education through games; whereas, organisations are offered guides and toolkits. Thus, the medium of communication used to deliver cyber-security awareness and education should be well suited to the particular target audience.

Fourthly, it is evident that the environment in which the awareness-raising and education take place would differ for each target audience. Again using the same example of children and organisations, children can be reached in schools and homes; whereas organisations can only be reached in the workplace. Therefore, the environment should be taken into consideration when developing cyber-security awareness and education campaigns and programmes – because this may influence the approach and/or tools to be used by the campaign or programme [43] [48] [49].

Finally, within the analysed cyber-security awareness and education initiatives, there are definite role-players. It is clear that cyber-security awareness is a shared responsibility; and everyone enjoying the cyberspace has a role to play. This is evident, since in all the countries studied, the governments were core in leading and resourcing cyber-security awareness and education.

In addition, industry has also assumed some of the responsibility, and has partnered with government [37] [38] [39] [40]. As such, when planning cyber-security awareness and education campaigns and programmes, the role-players should be identified, and their respective responsibilities should be clearly defined. Moreover, partnerships with relevant stakeholders should ideally be formed.

### 4.5 When can the implementation of cyber-security awareness and education initiatives be expected?

All four countries have implemented a set of cyber-security awareness and education-control measures. As far as the UK and Canada are concerned, 2015 is the year in which all cyber-security objectives should be accomplished; this includes awareness and education [37] [42]. It is indeed promising that both of these countries aim to have fostered a culture of cyber-security among their citizens by 2015, as both countries have

already taken definite steps in this regard to promote awareness and education. In addition, Canada is committed to generating periodic status reports, in order to monitor its progress more closely [42].

In the US, the NICE strategic plan makes no mention of a particular timeframe, in which its cyber-security awareness and education objectives will be accomplished [39]. However, it has defined a number of success indicators. Having both individuals and organisations understand online safety measures, and being encouraged to act securely online should serve as an indication that NICE has accomplished its aim. This approach suggests that in the US, cyber-security awareness and education are ongoing processes that will continue until the established indicators have materialised.

It is evident that these countries have in some way defined benchmarks that should assist them in evaluating the progress they have made towards accomplishing their goals. It can, therefore, be concluded that there should be some sort of monitoring and evaluation of the progress made in these cyber-security awareness and education efforts.

Cyber-security awareness and education comprise indeed a cross-cutting matter that warrants diligent handling. The government should take the lead in this regard; and, accordingly, establish national and international partnerships that would encourage all users of cyberspace to play their part.

This section has provided a discussion on the analysis in terms of the deductions and conclusions that were made, based on the questions posed at the beginning of this section. Based on the arguments, deductions and conclusions from the analysis, certain key factors were extrapolated for the purpose of constructing the basis of the proposed awareness and education framework for South Africa.

These key factors are listed below:

- Cleary articulated *goals* should be defined.
- A *dedicated team/group* should be appointed.
- An *action plan* should be outlined.
- A *national cyber-security awareness and education campaign* should be defined.
- *Partnerships* should be established.
- *Resources* should be in place.
- *Monitoring techniques* should be defined.

The above listed key factors form the basis of the proposed awareness and education framework. The resultant framework is presented in the following section.

# 5 THE CYBER-SECURITY AWARENESS AND EDUCATION FRAMEWORK

The previous section presented the key factors identified that should form the basis of the proposed cyber-security awareness and education framework. Moving forward, this section will introduce the proposed framework and discuss its elements individually.

The proposed framework is divided into five layers, and one overarching component, as listed below:

**The Strategic Layer**. This layer reflects the overall vision of the government concerning cyber-security awareness and education.

**The Tactical Layer**. This layer suggests the schemes that SA should employ to realise its cyber-security awareness and education goals.

**The Preparation Layer**. This layer prepares the contents of the scheme identified in the tactical layer.

**The Delivery Layer**. This layer defines the recipients of the preparations made in the preparation layer, namely: the target audience.

**The Monitoring Layer**. This layer examines the progress made by the scheme towards fulfilling the government's vision.

**Resources**. This component defines the resources, which should comprise the inputs in all the aforementioned layers.

Respectively, the abovementioned layers illustrate six themes embodied in the cyber-security awareness and education framework. Firstly, the cyber-security awareness and education 'dream' of the government; secondly, the proposed strategies to be used to fulfil the dream; thirdly, the preparations necessary for realizing this dream; fourthly, the heirs of the dream; fifthly, the monitoring of the progress towards the dream; and finally, the necessary resourcing.

A graphical illustration of the framework is presented in Figure 1. The remainder of this section will provide a detailed discussion on the respective layers of the framework.

## 5.1 The strategic layer

The strategic layer reflects the overall vision (the dream) of the government concerning cyber-security awareness and education. It is known from the draft Cyber-Security Policy that SA's overall vision, as far as cyber awareness and education are concerned, comprises a cyber-security culture. In this layer, this vision is delineated into three components: the national cyber-security policy, the responsible unit, and the strategic plan.

The first component is the national cyber-security policy detailing the primary objective of each country concerning cyber-security awareness and education. The second component is a responsible unit, a dedicated administration for cyber-security awareness and education. The responsible unit component proposes three ways in which this administration could be formed. These are listed below:

- Forming a new administration;
- Using one or multiple government departments; and/or
- Delegating to a private organization.

The framework recommends that once an administration is appointed, a comprehensive strategic plan should be drafted; hence the last component, the strategic plan. This plan should clearly articulate how SA should approach cyber-security awareness and education.

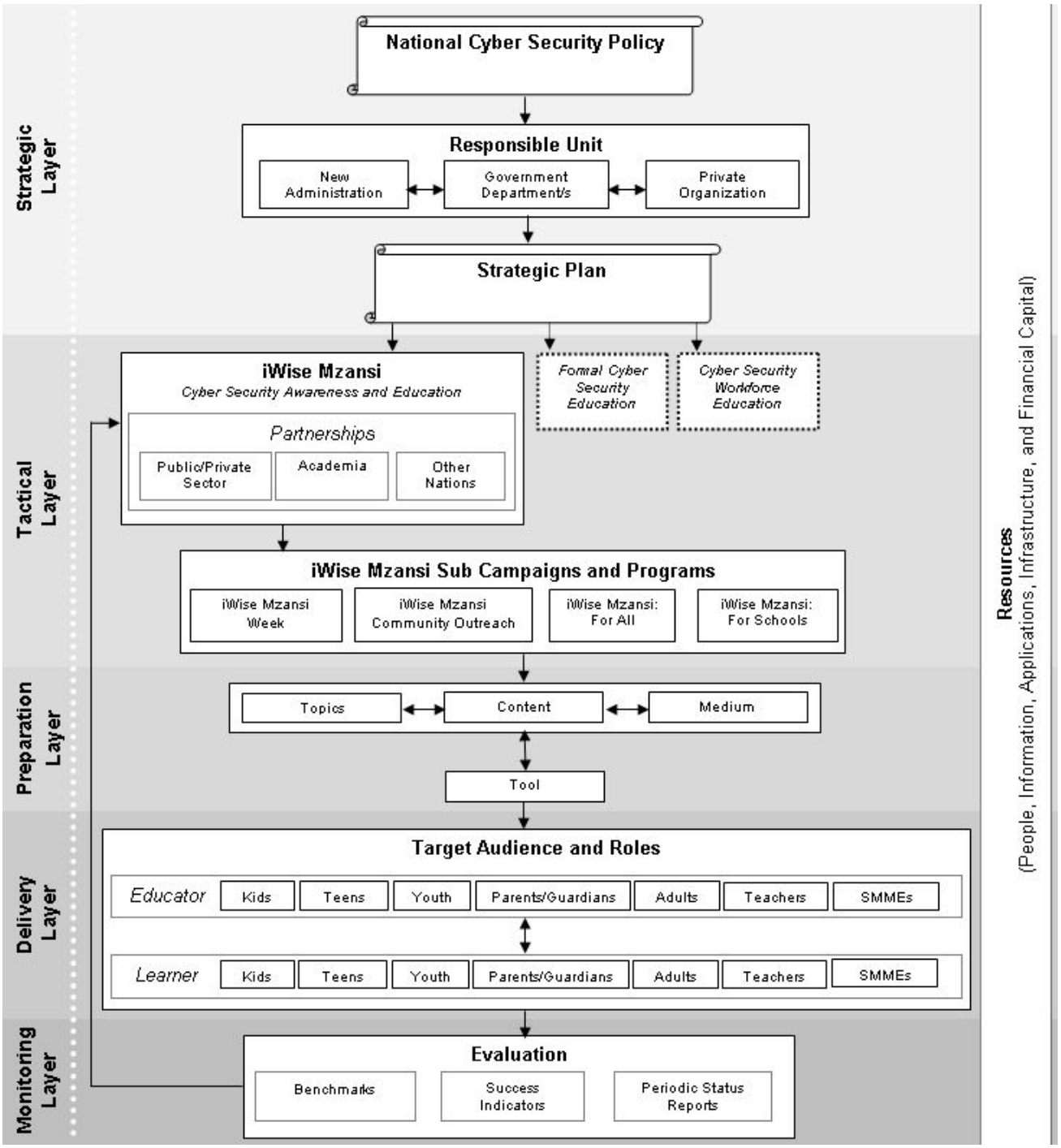


Figure 1: Cyber-security awareness and education framework

It is recommended that this plan should consider the South African context, taking into consideration other legislation that might influence the content of the plan. It was, however, beyond the scope of this study to elaborate on every aspect, which the strategic plan should comprise. Yet, from the analysis performed, it was gathered that the strategic plan should make known the schemes that the country should employ to realise its cyber-security goals. These schemes will fall into the next layer, which will be discussed in the following subsection.

## 5.2 The tactical layer

The tactical layer lies below the strategic layer. As stated, this layer continues where the strategic plan defined in the strategic layer has left off. In this layer, the suggested elements to drive cyber-security awareness and education are stated.

The tactical layer has four components, which are proposed in the framework. The first component is a national cyber-security awareness and education campaign. This suggestion was confirmed by the fact that all the countries analysed have one or more cyber-security awareness and education initiatives or campaigns. The proposed name for such a South African campaign is: *iWise Mzansi*. *iWise Mzansi* suggests an informative SA, hence the "i", and cyberwise SA, hence the name Mzansi. "Mzansi" is an accepted name that refers to SA.

The idea is for *iWise Mzansi* to be an overarching campaign that includes all sub-campaigns and initiatives.

The findings from the performed analysis indicate a variety of aspects, which should be considered in such a campaign. One of those aspects is the establishment of partnerships with the public and private Sectors, academia and other nations. These partnerships would allow industry, academia and other nations to contribute to a SA's cyber-security awareness and education endeavours. Such partnerships, particularly those with other nations, would promote the alignment of cyber-security awareness and education among nations.

Moreover, in partnership with academia, *iWise Mzansi* would benefit current research that could help to align what the campaign has to offer with the specific needs of South African citizens. It is proposed that *iWise Mzansi* could reach the people of SA through sub-campaigns and initiatives that could include the following:

- *iWise Mzansi* Week
- *iWise Mzansi* Community Outreach
- *iWise Mzansi* For All
- *iWise Mzansi* For Schools

*iWise Mzansi* Week is proposed to be an annual event aimed at all South African citizens. This week should serve as a reminder that cyber-security is a shared responsibility; and it should also induce and spread awareness of current and anticipated cyber-security practices and issues. With all these campaigns, a South African 'flavour' should be adopted, meaning the South African context should be taken into consideration.

This week could adopt and further expand on the National Cyber-Security Awareness Week hosted by SACSAA.

*iWise Mzansi* Community Outreach is proposed to give everyone an opportunity to lend a helping hand. This programme would allow any member of society to be part of *iWise Mzansi*, by volunteering to participate in spreading the cyber-security awareness and education message to communities. This programme is closely linked with the well-known philosophy of *ubuntu* (humility) in SA [50].

It is proposed that *iWise Mzansi* For All could be an all-encompassing website addressing all groupings of the South African society, as well as SMMEs. It is proposed that this website provide up-to-date information that would equip its audience with the necessary cyber-security information, in order to create knowledgeable South Africans. The topics covered in the website should be tailored and delivered in a manner that is best suited to the general public and employees of SMMEs.

Topics identified in the analysis include, but are not limited to, cyber-bullying, cyber-stalking, identity-theft, fraud, phishing, securing personal and private information online, and secure behaviour.

Finally, it is proposed that *iWise Mzansi* For Schools should target learners in primary and secondary schools. This campaign should ensure that cyber-security forms part of the school curriculum, and that awareness and education are delivered to the scholars in a manner that is suitable for each age group.

It is worth noting that *iWise Mzansi* is not intended to replace the campaigns that are already active in SA, but rather to unite everything together under one unique truly South African effort.

Since cyber-security education is broad in nature, a national cyber-security awareness and education campaign is not the only aim to attain. Alongside *iWise Mzansi*, there are two further components: formal cyber-security education for students, and cyber-security education for those in the workforce.

However, providing insight on what these two components should consist of falls outside of the scope of this paper. Thus, students, together with people in the workforce, are also part of society; therefore, they should be included in *iWise Mzansi*.

The major facet of the tactical layer is the cyber-security awareness and education campaign, *iWise Mzansi*, and also the suggested subordinate campaigns and programmes that should be used to reach South African citizens. Having said this, the following questions must be asked:

- What topics should *iWise Mzansi* cover?
- What communication tools should be employed?

The following subsection will introduce another layer that should answer the questions posed above.

## 5.3 The preparation layer

The preparation layer concerns itself with defining the cyber-security awareness and education resources that *iWise Mzansi* would offer to the people of SA. The preparation layer comprises four components: topics, content, medium and tools. With regard to topics, from the analysis of cyber-security awareness and education initiatives, a number of topics that are common throughout the initiatives may be identified. Such topics include, but are not limited to: cyber-bullying, cyber-stalking, identity-theft, fraud, phishing, securing personal and private information online, and secure behaviour. These topics and more could be covered by *iWise Mzansi*. However, further research needs to be done, in order to discover the particular needs of South African citizens.

Figure 1 suggests a particular relationship between content and topics in the preparation layer. This relationship is guided by the target audience to which the material will be offered. For example, if material on cyber-bullying is offered to children, the content might include 'how to report a cyber-bully'.

However, the same topic, offered to a different target audience, such as a parent, could include such content as 'the warning signs of a cyber-bullied child'. Thus, there is a definite link between topic and content.

The preparation layer, as shown in Figure 1, further presents a link between content and medium. This relationship suggests that based on the defined topic together with the content, a suitable medium of communication should be chosen. There are two acknowledged mediums: paper based and electronic. Once these elements are clear, the tools to be used must be defined. These tools include: websites, videos, games, quizzes, and so forth. Thus, a suitable tool should be chosen, based on the topic, content and medium. From this layer, one further question arises:

- To which target audience would *iWise Mzansi* deliver cyber-security awareness and education?

This question will be addressed in the following subsection.

## 5.4 The delivery layer

The delivery layer concerns itself with the process of defining the target audience to which *iWise Mzansi* will deliver awareness and education. In addition, it will also define the roles that this audience would play within *iWise Mzansi*, and amongst each other. There could possibly be seven different target audiences defined, namely:

- Children younger than 13 years
- Teenagers
- Youths
- Parents/Guardians
- Adults
- Teachers
- Small, Medium and Micro-sized Enterprises (SMMEs)

It is proposed in this layer that *iWise Mzansi* deliver cyber-security awareness and education to the abovementioned audiences, since they represent the nation at large. In addition, this layer identifies two roles that these audiences should play, namely: a Learner Role and an Educator Role.

It is well known that cyber-security is the responsibility of everyone who enjoys the benefits offered by cyberspace. Therefore, it is recommended that the defined target audience accept the responsibility of using the resources that *iWise Mzansi* offers to educate them, thereby assuming the role of a learner. Moreover, it is also recommended that everyone passes on what they have learnt to one another, thereby assuming the role of an educator.

Once the target audiences and roles in *iWise Mzansi* are clear, all that is left is to define the manner in which the progress towards achieving the primary cyber-security awareness and education is to be monitored. The monitoring component will be discussed in the following subsection.

## 5.5 The monitoring layer

The Monitoring Layer is the final layer of the cyber-security awareness and education framework. It was gathered from the analysis that there should be monitoring and evaluation of the progress made in the cyber-security awareness and education efforts. In addition, the effectiveness of the campaign should be evaluated. As such, the framework suggests the following:

- Benchmarks must be declared
- Success indicators must be defined
- Periodic status reports must be generated

It is suggested that the feedback from the evaluation should inform *iWise Mzansi* in the tactical layer. In so doing, this national cyber-security awareness and education campaign should be adapted – on the basis of the feedback from the evaluation. For instance, if a declared benchmark or certain success indicator fails to materialise, *iWise Mzansi* may possibly need to make some changes in the Preparation Layer. Consequently, the topics, content or tools in this layer may be adapted, in order to achieve the expected results.

The monitoring layer serves as the last layer of the framework. The following subsection will discuss the resources component.

## 5.6 Resources

In order for all the components identified in the framework within each layer to be addressed, certain resources have to be in place. The framework identifies five types of resources that would be needed as input in all the layers of the framework. These resources are as follows:

**People**. The people needed to carry out a certain function.

**Information**. The information required to carry out a particular function.

**Applications**. Computer applications, such as software programs, which will be needed.

**Infrastructure**. The physical hardware, such as desktops and servers.

**Financial Capital**. The monetary resources that will be needed.

These resources are adopted from the Information Technology Infrastructure Library (ITIL), and have been identified as being essential in delivering an information technology service [51]. In the context of this framework, cyber-security awareness and education comprise the service to be delivered. Therefore, within the five layers of the framework, appropriate resources have to be identified.

Each and every layer of the cyber-security awareness and education framework will need one or more resources, in order for the components within each layer to be in place. Hence, the government has the duty to ensure that these resources are in place. This subsection marks the last component of the proposed framework.

The proposed framework was developed in such a manner that its layers are in line with the Plan-Do-Check-Act (PDCA) cycle presented by Figure 2.

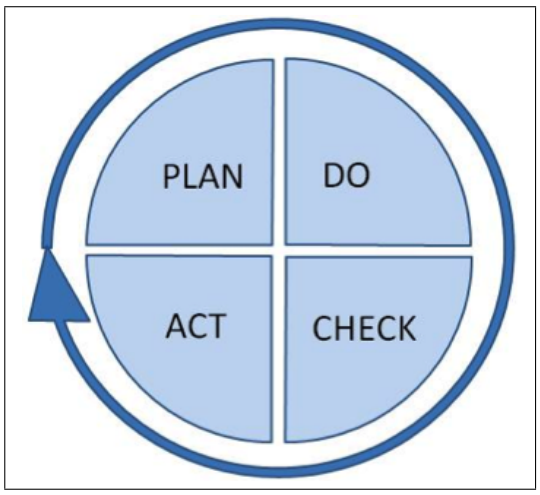


Figure 2: PDCA cycle

Figure 2 depicts the iterative four-step process of the PDCA Cycle. According to ISO/IEC 27000, these steps signify the following [52]:

**Plan**. Establishing objectives and processes, which are necessary, in order to deliver certain outcomes.

**Do**. Implementing the outlined plan.

**Check**. Monitoring and measuring progress against particular requirements.

**Act**. Taking action, in accordance with the feedback obtained from the monitoring.

These steps overlap well within the layers of the proposed framework. The planning step can be recognised in the strategic and tactical layers. It was elaborated on in Subsection 5.1 how the strategic layer reflects the overall vision of SA concerning cyber-security awareness and education. As part of the planning step, the vision is delineated into clearly defined objectives. The objectives are to form a dedicated administration for cyber-security awareness and education, including drafting a comprehensive strategic plan that would clearly articulate how SA should approach cyber-security awareness and education.

The planning phase extends to the tactical layer – by declaring the elements that are proposed to drive cyber-security awareness and education in SA. These elements are: *iWise Mzansi* Formal Cyber-Security Education and Cyber-Security Workforce Education.

The doing step manifests in the preparation and delivery layers. In the preparation layer, the resources that *iWise Mzansi* will offer to its targeted audience are defined. The doing step then overlaps with the deliver layer, since the actual target audience is defined by the prescribed roles.

The monitoring layer encapsulates both the checking and acting phase of the PDCA cycle. It is suggested in this layer that the progress made in the cyber-security awareness and education efforts be monitored and evaluated against certain benchmarks and success indicators. Thereafter, the feedback that should be obtained from monitoring and evaluation would trigger the acting step, as elaborated in Subsection 5.5 of this paper.

The use of this proposed framework should enable SA to define a national cyber-security awareness campaign, here proposed as *iWise Mzansi*. This campaign would serve as a means for providing SA citizens with the necessary cyber- security understanding and knowledge, and would, therefore, contribute to the creation of the envisaged culture.

## 6 VERIFICATION OF THE FRAMEWORK

In Section 3 it was mentioned that the framework was verified by using elite interviews. As such, this section seeks to discuss the verification of the proposed cyber-security awareness and education framework for SA. Included in this section, is how the comments from the elites were addressed.

A week prior to conducting the elite interview, an interview brief was sent to the elites. The interview brief aimed to introduce the framework, and also to provide some background on the form of the interview to be conducted. This was done, in order to allow the elites to understand what was expected of them.

Before interviewing the elites, the proposed cyber-security awareness and education framework was presented in the form of a PowerPoint slide show. This presentation was intended to elaborate on the underlying research that forms the basis of the proposed framework. In addition, all the layers and components of the proposed framework were presented in detail, so that the elites could have a clear understanding of the context. Subsequently, the actual elite interview was conducted.

As previously mentioned, elite interviews are semi-structured; and they do not call for standardised questions. However, in this case, the questions were fairly standard; and both elites were asked the same ques-

tions. Nevertheless, even though the questions were fairly standard, with this choice of interview, the researcher had the opportunity to probe the information provided by the elites.

The questions, which were posed, are listed below:

- Do you agree with the layers of the proposed framework?
- Do you agree on the components of the proposed framework?
- Is the framework comprehensive enough?
- Do you think the framework would contribute to the cultivation of the suggested culture?
- Are there any other frameworks of which you are aware, to which you can refer me?
- Any other comments and suggestions?

The above questions were intended to verify the layers, components and comprehensiveness of the proposed cyber-security awareness and education framework. Furthermore, what was essential was to obtain confirmation from the elites that the proposed framework would contribute to cyber-security.

The interview was audio-taped using a mobile phone. The audio tape was then transcribed accordingly.

Concerning the five layers of the framework, both elites approved these layers; and one of the elites expanded by saying:

> Yes, I do agree with the layers of the framework, one of the phases of any awareness that we always have, which I have picked up from various studies is that others have three; while others have two. These phases are preparation phases, followed by the design phase; and then you have the implementation phase, and your review phase, for your monitoring...

When asked whether they agreed with the components of the proposed framework, the elites suggested additional concepts. Elite one suggested that guardians be added as a target audience in the delivery layer. As suggested, the framework was revisited and adapted accordingly. Additionally, elite two suggested that there be a relationship indicator in the 'responsible unit' component found in the strategic layer, in order to portray the interrelatedness of government departments. The framework was adapted, as advised.

In terms of the comprehensiveness of the framework, both elites confirmed that the proposed framework was indeed comprehensive; and one of the elites expanded by saying:

> I would say it's comprehensive, because for any awareness campaign, there must be these components: goal/purpose, objective of the campaign, the need of the campaign, campaign name, target audience, delivery methods, and evaluation.

In addition, the elites were positive about the contribution the proposed cyber-security awareness and education framework would make to the cyber-security culture envisaged by SA.

> The framework will contribute to cyber-security awareness and education, because it structures things that people are currently doing: a little bit here and there, things that people don't see as a full-blown framework. The framework nicely links all these facets.

Regarding other existing frameworks, none of the elites could make reference to an existing framework. Finally, when the elites were asked whether they had any other comments and suggestions, both elites had some concerns. Elite one was against allowing children to assume the role of being educator (see Subsection 5.4). However, in the UK, peer-to-peer education is recommended, as it is believed that children more easily learn and accept input from their peers [6]. Thus, this comment was overlooked.

Elite two suggested that Estonia be added to the developed countries, which were analysed in Section 4. The criteria used to select the developed countries that were studied are made known in Section 4. However, in the case of Estonia, some of the documentation deemed important to the study, needed to be translated – before being used. This was a disadvantage, primarily because the integrity of the information would come into question. Therefore, Estonia was not included as a participant in the comparative analysis.

Based on the feedback received from the elites, it can be concluded that the proposed framework was sufficiently validated. Moreover, the demonstration and evaluation steps, as part of a design science approach were conducted satisfactorily. Therefore, it could be argued that the cyber-security awareness and education framework is basically sound.

## 7 CONCLUSION

Cyberspace had humble beginnings. Over time, it has progressed immensely – providing individuals with endless opportunities. Embedded in these opportunities, however, are risks that compromise the safety and security of the individuals that participate in cyberspace. It would seem that people are largely unaware of these risks; and so they put themselves, as well as businesses and governmental assets and infrastructure, at risk.

In recognition of this, SA wishes to promote a culture of cyber-security among its citizens. Cyber-security awareness and education together play a big role in cultivating such a culture. Accordingly, this paper proposes a cyber-security awareness and education framework that would assist SA in promoting its envisaged cyber-security culture.

The implementation of this framework would afford SA a national cyber-security awareness campaign: *iWise Mzansi*. Furthermore, making use of its subsidiary campaigns would mean that South African citizens could be the recipients of cyber-security awareness and education, suited to a South African audience.

## ACKNOWLEDGMENTS

The authors hereby acknowledge the financial assistance of the National Research Foundation (NRF) towards this research. Opinions expressed and conclusions arrived at, are those of the authors and not necessarily the NRF.

## REFERENCES

[1] E. Kritzinger and S. H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement". *Computers & Security*, vol. 29, no. 8, pp. 840–847, 2010.

[2] A. Riem. "Cybercrimes of the 21st Century". *Computer Fraud & Security*, vol. 2001, no. 4, pp. 12–15, 2001.

[3] A. De Joode. "Effective corporate security and cybercrime". *Network Security*, vol. 2011, no. 9, pp. 16–18, 2011.

[4] K.-L. Thomson, R. von Solms and L. Louw. "Cultivating an organizational information security culture". *Computer Fraud & Security*, vol. 2006, no. 10, pp. 7–11, 2006.

[5] M. De Lange and R. Von Solms. "The importance of raising e-safety awareness amongst children". In *Proceedings of the 13th annual conference on World Wide Web applications*, p. 14. 2011.

[6] S. Atkinson, S. Furnell and A. Phippen. "Securing the next generation: enhancing e-safety awareness among young people". *Computer Fraud & Security*, vol. 2009, no. 7, pp. 13–19, 2009.

[7] M. de Lange and R. von Solms. "An e-Safety educational framework in South Africa". In *Proceedings of the Southern Africa Telecoms and Network Applications Conference*. 2012.

[8] K. D. Mitnick and W. L. Simon. *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2001.

[9] E. Kritzinger and S. H. von Solms. "A framework for cyber security in Africa". *Journal of information assurance and cybersecurity*, vol. 2012, 2012. doi: 10.5171/2012.322399.

[10] J. Christensen. "Solving the cyber security problem: The role of the Department of Homeland Security", 2003.

[11] E. Kritzinger and K. Padayachee. "Engendering an e-safety awareness culture within the South African context". In *AFRICON, 2013*, pp. 1–5. IEEE, 2013.

[12] Z. Dlamini and M. Modise. "Cyber security awareness initiatives in South Africa: A synergy approach". *Case studies in information warfare and security: For researchers, teachers and students*, p. 1, 2013.

[13] N. Kortjan and R. Von Solms. "Fostering a cyber security culture: A case of South Africa". In *2012 Conference*. 2012.

[14] Government of South Africa. "South African government gazette: Draft cybersecurity policy of South Africa", 2010.

[15] Government of South Africa. "South African government gazette: Draft National Cybersecurity Policy Framework for South Africa", 2011.

[16] M. Grobler, Z. Dlamini, S. Ngobeni and A. Labuschagne. "Towards a cyber security aware rural community". In *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference. Hayatt Regency Hotel, Rosebank, Johannesburg, South Africa 15 - 17 August 2011*. 2011.

[17] South Africa Cyber-Security Academic Alliance. "Welcome to SACSAA", 2014. URL `http://www.cyberaware.org.za`.

[18] Cyber-Security Awareness Project. "Be aware, be cyberaware", 2014. URL `http://eagle.unisa.ac.za/elmarie/`.

[19] CSIR. "Media release: Be careful of what you share online, CSIR warns", October 2012. URL `http://goo.gl/5rNe7P`.

[20] A. R. Hevner, S. T. March, J. Park and S. Ram. "Design science in information systems research". *MIS quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[21] K. Peffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen and J. Bragge. "The design science research process: A model for producing and presenting information systems research". In *Proceedings of the first international conference on design science research in information systems and technology (DESRIST 2006)*, pp. 83–106. 2006.

[22] E. Hofstee. *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule*. EPE, 2006.

[23] M. Mills, G. G. Van de Bunt and J. De Bruijn. "Comparative research persistent problems and promising solutions". *International Sociology*, vol. 21, no. 5, pp. 619–631, 2006.

[24] N. Kortjan and R. von Solms. "Cyber security education in developing countries: A South African perspective". In *e-Infrastructure and e-Services for Developing Countries*, pp. 289–297. Springer, 2013.

[25] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee. "A design science research methodology for information systems research". *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[26] D. R. Cooper, P. S. Schindler et al. *Business research methods*. McGraw-Hill/Irwin New York, NY, 2003.

[27] J. L. Hochschild. "Conducting intensive interviews and elite interviews". In *Workshop on Interdisciplinary Standards for Systematic Qualitative Research*. National Science Foundation, 2009.

[28] C. Marshall and G. B. Rossman. *Designing qualitative research*. Sage, 5th ed. edn., 2011.

[29] O. Tansey. "Process tracing and elite interviewing: a case for non-probability sampling". *PS: Political Science & Politics*, vol. 40, no. 04, pp. 765–772, 2007.

[30] H. Zuckerman. "Interviewing an ultra-elite". *Public Opinion Quarterly*, vol. 36, no. 2, pp. 159–175, 1972.

[31] L. McDowell. "Elites in the City of London: some methodological considerations". *Environment and Planning*, vol. 30, no. 12, pp. 2133–2146, 1998.

[32] K. Smith. "Problematizing power relations in elite interviews". *Geoforum*, vol. 37, pp. 643–653, 2006.

[33] R. Mikecz. "Interviewing elites addressing methodological issues". *Qualitative inquiry*, vol. 18, no. 6, pp. 482–493, 2012.

[34] J. A. Conti and M. O'Neil. "Studying power: qualitative methods and the global elite". *Qualitative Research*, vol. 7, no. 1, pp. 63–82, 2007.

[35] OECD. "The Organisation for Economic Co-operation and Development", n.d. URL `http://www.oecd.org/about/`.

[36] The White House. "Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure", 2009. URL `http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf`.

[37] UK Government Cabinet Office. "The UK cybersecurity strategy: Protecting and promoting the UK in a digital world", 2011.

[38] Government of Canada. "Canada's cyber-security strategy".

[39] National Initiative for Cybersecurity Education. "National Initiative for Cybersecurity Education strategic plan", 2012.

[40] Commonwealth of Australia. "Cyber-security strategy", 2009.

[41] Commonwealth of Australia House of Representatives. "Hackers, fraudsters and botnets: Tackling the problem of Cyber Crime", 2010.

[42] Government of Canada. "Action plan 2010-2015 for Canada's cyber-security strategy", 2010.

[43] Department of Broadband Communications and Digital Economy. "Stay smart online", n.d. URL `http://www.staysmartonline.gov.au`.

[44] Department of Homeland Security. "Stop. Think. Connect.", 2012. URL `http://www.dhs.gov/stopthinkconnect`.

[45] Department of Homeland Security. "Stop. Think. Connect. Friends of the campaign program.", 2012. URL `http://www.dhs.gov/stopthinkconnect-friends-campaign-program`.

[46] Public Safety Canada. "Get cyber safe", 2013. URL `http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx`.

[47] Get Safe Online. "Get Safe Online partners", 2012. URL `https://www.getsafeonline.org/partners-and-supporters/`.

[48] Australian Competition and Consumer Commission. "ScamWatch", 2013. URL `http://www.scamwatch.gov.au/content/index.phtml/itemId/693900`.

[49] Australian Communications and Media Authority. "Cyber smart", 2013. URL `http://www.cybersmart.gov.au`.

[50] T. Murithi. "Practical peacemaking wisdom from Africa: Reflections on Ubuntu". *The journal of Pan African studies*, vol. 1, no. 4, pp. 25–34, 2006.

[51] S. Taylor, V. Lloyd and C. Rudd. "ITIL Version 3 Service Design". *The Office of Government Commerce*, 2011.

[52] ISO/IEC 27000. "ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems - Overview and vocabulary (third edition)", 2009. URL `http://www.iso27001security.com/html/27000.html`.