Cyber Security Awareness Initiatives in South Africa: A Synergy Approach

Abstract: Technological advances have changed the manner in which ordinary citizens conduct their daily activities. Many of these activities are carried out over the Internet. These include filling tax returns, online banking, job searching and general socialising. Increased bandwidth and proliferation of mobile phones with access to Internet in South Africa imply increased access to Internet by the South African population. Such massive increased in access to Internet increases vulnerabilities to cyber crime and attacks and threatens the national security. As a result, South Africa remains one of top three countries that are targeted by phishing attacks, the other two are the US and the UK (RSA, 2011). As a response, various entities engage in cyber security awareness initiatives and trainings with the aim to create cyber security awareness (CSA) among the citizens of South Africa. In the absence of a national cyber security policy, however, these awareness initiatives and programmes are delivered through a variety of independent mechanisms. Various entities engage in cyber security awareness training each with its specific objectives and focus areas. It is argued in this paper that cyber security is complex and multi-faceted. No single solution can effectively address it. While the current means to create cyber security awareness does make impact, the fragmented and uncoordinated nature thereof have a potential to create its own dynamics. The focus of organisations to deliver on their own objectives translates to some extent into the optimisation of the behaviour of individual entities as opposed to the optimisation of the national cyber security awareness as a whole. This paper evaluates the extent to which the current cyber security awareness initiatives address the cyber security threats and risks. The assessment is based on the initiatives objectives, alignment of the programme to the cyber threats, and the target audience.

Keywords: National security, cyber security awareness, cyber fraud, cybercrime, cyber threats

1 Introduction

Security and protection of individuals and organisation against the fast growing dangers of the cyber crime remain one of the major challenges facing cyber security experts, scholars and politicians. Cyber crime is on the rise in South Africa (SAPS, 2011). The increase is the result of the increased bandwidth and the proliferation of smart phones which has widened access to Internet to the majority of South Africans (RSA, 2011). Sixteen percent of the cyber crime victims were affected through their phones compared to only 10 percent globally. Malware and computer viruses made up the biggest portion of cyber crime in South Africa. Scams and phishing fraud made up the rest. The total net cost of cyber crime in South Africa is estimated at R10.9 billion (Ferrier Int., 2011), making up one percent of the global net cost of R2.9 trillion. Cyber security awareness is the first line of defence against cyber attacks.

In South Africa, cyber security awareness initiatives are delivered through a variety of independent uncoordinated mechanisms. Various entities are engage on cyber security awareness training each with their specific objectives and focus areas. The cyber security is complex and multi-dimensional. An effective approach is that which accommodates and integrates all the dimensions. Therefore, the effectiveness of the current initiatives to the delivery of cyber security awareness initiatives that are relevant needs to be evaluated. The study outlines, evaluates and assesses the relevance of current cyber security initiatives in addressing cyber security challenges facing South Africa.

To achieve its aims, the paper is structured as follows: Section 2 defines key concepts of Information Security field and subsequently identifies the most prevalent cyber crime in South Africa. This is followed by Section 3 which identifies and describes current cyber security awareness initiatives in South Africa with specific reference to key questions that must be addressed by any cyber security awareness programme, the goals and objectives of individual initiatives, the group that is targeted, and the delivery method. The analysis of the relevance and effectiveness of the initiatives is based on how well the initiative responds to the challenges, alignment between the target group most attacked and those targeted for the initiatives. Section 4 concludes and presents future works.

2 Definition of key concepts

This section discus some of the significant concept in Information Security field and this study, these include: cyberspace, cyber crime and cyber security.

2.1 Cyberspace

Cyberspace refers to a physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, networks, and their computer programs, computer data, content data, traffic data, and users (IST-Africa, 2011).

Here are some of the threats associated with Internet or cyberspace that make cyber crime complex and difficult to eradicate (SAPS, 2011):

- *Cyber attacks are indirect:* Through cyberspace, nation-states can perpetrate espionage; industrial spies can steal trade secrets; criminals can steal money; and militaries can disrupt command-and-control communications.
- *Cyberspace or Internet is everywhere:* Today all business activities including production, manufacturing, transportation, telecommunications is heavily dependent on the Internet. There is a drive in South Africa to integrate all its government services' systems, such as home affairs, SARS (South African Revenue Service) and commercial banks.
- *The Internet has no boundaries*: the natural structure of Internet is complex and not easy to manage. This requires cooperation amongst all nations as one leak can be a threat to innocent users, who are not even residing where the leak was started or targeted (DiGregory, 2000).
- *Anonymity:* Everyone can be anyone they choose to become when they are online. Despite age or race, Internet, its applications and services, it is easy to lie about anything; this has resulted in high rate of children abduction, and women abuse all over the world (Fick, 2009).

Since the users of cyberspace span across all the layers of the society, so does cyber attacks and therefore a comprehensive and integrated approach is required for the security of the citizens of any country.

2.2 Cyber crime

The draft of South African National Cybersecurity Policy defines cybercrime as illegal acts, the commission of which involves the use of information and communication technologies (South African Government Gazette, 2010).

2.2.1 Cyber crime in South Africa

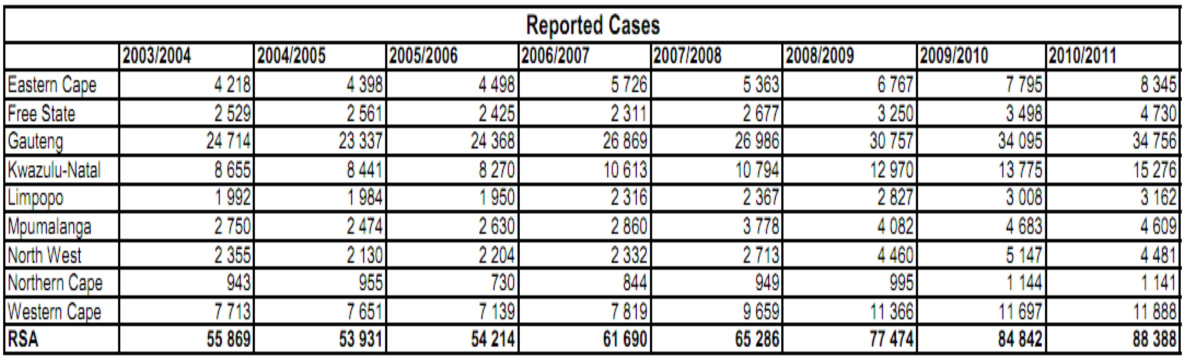
Globally the US is the top hosting country for phishing attacks, that is, two out of every three phishing attacks that are identified. The countries that have consistently been among the top five hosts over the last six months include the US, UK, Canada, Germany and South Africa (RSA, 2011).

Business Against Crime from South Africa indicated that incidents of commercial crime involving computers had risen by 13% to 61 690 per 100 000 people between 2007 and 2008 (Ferrier Int., 2011). In 2011 alone, 84% of the South Africans who responded to Norton survey said they have been victims of cyber crime (France24, 2011). Online Fraud Report (October 2011) noted that South Africa remains among the 'top 5 attacked countries in the world' in terms of phishing attack volume in September (RSA, 2011). In February 2011, an estimated 18,079 phishing attacks were discovered to be aimed at South African networks, which accounts to an 11% increase from January, this was for the first time in nearly a year, that the total number of phishing attacks in a single month reached over 18,000 especially in South Africa. This makes phishing attacks the major cyber threat to South Africans (SAPS, 2011), (RSA, 2011).

The Crime Report 2010/2011 by South African Police Service (SAPS) also noted a steady increase is commercial crime in South Africa (SAPS, 2011). It is worth noting that computer or cyber crime is not explicitly singled out in this report but is seen as part of commercial crime. Commercial crime refers to any offence against statutory provisions which customs are responsible for enforcing, committed in order to either avoid payment of responsibility duties on movements of commercial goods; or any restrictions applicable to commercial goods; or receive any repayments, subsidies or other disbursements to which there is no proper entitlement; or illicit commercial advantage injurious to principle and practice of legitimate business competition (World Customs Organization, 2011).

This definition is open and encompasses many other illegal activities, which are mainly not cyber crime. If cyber crime is not specified and rated with various crimes that the country experience, the continuous increasing rate of cyber crime should be expected. This is shown in Table 1. The Table shows that there was a slight decrease in number of reported cases of commercial crime from 55 869 to 53 931 for the years 2003/2004 and 2004/2005. The years 2006 – 2011 have shown a consistent increase. Furthermore, Gauteng and the hub of economic activity has consistently remained the province with the highest reported cases since 2003.

Table 1: Commercial crime in RSA from 2003/2004 to 2010/2011 (SAPS, 2011)



	Reported Cases							
	2003/2004	2004/2005	2005/2006	2006/2007	2007/2008	2008/2009	2009/2010	2010/2011
Eastern Cape	4 218	4 398	4 498	5 726	5 363	6 767	7 795	8 345
Free State	2 529	2 561	2 425	2 311	2 677	3 250	3 498	4 730
Gauteng	24 714	23 337	24 368	26 869	26 986	30 757	34 095	34 756
Kwazulu-Natal	8 655	8 441	8 270	10 613	10 794	12 970	13 775	15 276
Limpopo	1 992	1 984	1 950	2 316	2 367	2 827	3 008	3 162
Mpumalanga	2 750	2 474	2 630	2 860	3 778	4 082	4 683	4 609
North West	2 355	2 130	2 204	2 332	2 713	4 460	5 147	4 481
Northern Cape	943	955	730	844	949	995	1 144	1 141
Western Cape	7 713	7 651	7 139	7 819	9 659	11 366	11 697	11 888
RSA	**55 869**	**53 931**	**54 214**	**61 690**	**65 286**	**77 474**	**84 842**	**88 388**

Cyber crime incidents increase in monetary value every day in South Africa. Here are some of the examples: The Road Accident Fund has been stolen via the use of key loggers, accounting to the value of R15 million; the ABSA bank electronic fraud incidents cost up to R30 million, Landbank's electronic incidents accounts to R150 millions and the South African Revenue Services (SARS) electronic fraud incidents to the value of R100 millions in the year 2010 (SA government gazette, 2010), (The New Age, 2011).

The cyber crime that remain on top of the list of South African major cyber attacks and threats remain to be phishing attacks, identity theft and monetary fraudulent on all levels of national society. Other cyber crime and security threats that have been experienced in South Africa includes: Adware, Botnet, Cyber bullying, Cyber stalking, Data Theft, Hacking, Hoax Email, Key logging, Malware, Social Engineering, Spam Spyware and Trojan Virus (ISG-Africa, 2011)

Although reduction of cyber crime received a special mention during his 2009 State of the Nation address, President J.Z. Zuma stated that "Amongst other key initiative, we shall intensify our efforts against cyber crime and identity theft, and improve systems in our jails to reduce repeat offending", cyber crime rate in South Africa continue to increase everyday and there are no proper structures yet to deal with it (Zuma, 2009).

2.3 Cyber security

Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user assets.

Although South Africa currently does not have a cyber security policy, it recognises the need for a policy that will reduce the vulnerability of cyberspace, prevention of cyber threats and attacks and the ability to recover swiftly from any attack. To date, there is only a draft of cyber security policy that was released in February 2010 and a national cyber security policy framework is still drafted. The next section therefore will outline key objectives of cyber security policies from various countries.

2.3.1 South African Cyber Security Policy

The SA Cyber security policy is made out of six key elements or strategic objectives to:

- Facilitate the establishment of relevant structures in support of cyber security;
- Ensure the reduction of cyber security threats and vulnerabilities;
- Foster cooperation and coordination between government and private sector;

- Promote and strengthen international cooperation on cyber security (SA government gazette, 2010).

2.3.2 US Cyber Security Policy

A US cyber security policy review team suggest that any complete national cyber policy must consider, at a minimum, the following elements:

- Governance: Encompasses US Government (USG) structures for policy development and coordination of operational activities related to the cyber mission across the Executive Branch.
- Architecture: Deals with performance, cost, and security characteristics of existing information and communications systems and infrastructures as well as strategic planning for the optimal system characteristics.
- Norms of Behaviour: Addresses elements of law, regulation, and international treaties and undertakings, as well as consensus-based measures.
- Capacity Building: Encompasses the overall scale of resources, activities, and capabilities required to become a more cyber-competent nation (Cyberspace Policy Review, 2011).

2.3.3 Kenya Cyber Security Policy

Kenyan cyber security policy is not ready yet. Currently, the following objectives are considered:

- Collaboration between stakeholders;
- Develop relevant Policies, Legal and Regulatory frameworks
- Establish national CERT thus providing a Trusted Point of Contact (TPOC);
- Build Capacity: technical, legal and policy;
- Awareness creation is key;
- Research and development;
- Harmonization of Cybersecurity management frameworks at the regional level (at the very least) (Ngudi, 2010).

2.3.4 Mauritius Cyber Security Policy

Mauritius is one of the few countries who have most of cyber security infrastructures in place, including response team, incident response team, the awareness portal the cybercrime prevention committee and cyber security strategy, which have the following as its objectives:

- National Awareness Programs and Tools
- Good Governance of Cyber Security & Privacy
- Harnessing the Future to Secure the Present
- Personal Cyber Security
- A holistic approach integrates many elements, (Carnegie Mellon CyLab, 2008).

Although national cyber security policies differ from country to country, the key objectives and the approaches are gearing towards the achievement of the similar goal with cyber security awareness as a common feature.

3 Cyber Security Awareness

Cyber security awareness (CSA) is the security training that is used to inspire, stimulate, establish and rebuild cyber security skills and expected security practise from a specific audiences (Ministry of Defence-Estonia, 2008). It used to promote and encourage Internet users to practise safety precautions, and train them on online defence methods. Furthermore, it equips these users with cyber security skills on all the aspects of cyber security so that not only the national network infrastructures are kept resilience to cyber attacks and threats, but also the users are well informed (Dlamini *et al.,* 2011).

Any cyber security awareness initiative should have a plan, clearly defined goals and objectives, expected results, delivery methods, risks, and methods to evaluation the initiative.

Peltier believes that in order for the cyber security awareness program to be successful, there are five key factors that need to considered and ensured (Peltier, 2005). These include:

- A clear process to take the message to the users or targeted audience in order to reinforce cyber security as a significant concept.
- Identification of the individuals who are responsible for the implementation of cyber security awareness program.
- Determination and evaluation of the sensitivity of information and the criticality of cyber security infrastructure, applications and systems.
- The reasons for the implementation of cyber security concepts and awareness programs in convincing the audience of the significance of cyber security awareness programs that must be implemented.
- Ensuring that the related government department or the management supports the goals and objectives of the cyber security awareness program for the community.

Therefore, any cyber security awareness initiative has to answer a number of key issues if it is to be viable. Some of these issues may include:

- The programme /strategy which provide a coherent analysis of the state of cyber crime and security and the sources of these conditions. This analysis must of course identify the positions and interest of the different players within such a context.
- The initiative must identify the target group whose interest it seeks to address and specify the goals of such a group regarding cyber security awareness.
- The programme must specify the implementation plan and the how its effectiveness will to be measured.

3.1 Cyber Security Awareness Initiatives in South Africa

The first part of this section identifies and describes the current Cyber Security Awareness (CSA) initiatives in SA. The research question for this part is *"do the initiatives/programmes contain the most basic requirement such as a plan, goals and objectives, delivery methods, etc.?"*

The second part evaluates the effectiveness of the initiatives/programme and the research question is *"Do the initiatives address the key issues making it viable?"*

3.1.1 Identification and description of CSA initiatives

A number of initiatives engaging in CSA have been identified. According to Grobler *et al*. (2011) the initiatives are spread across only four provinces (Gauteng, Mpumalanga, Limpopo, and Eastern Cape) out of the nine provinces in South Africa.

The list of these initiatives is summarized in Table 2 and Table 3. Table 2 demonstrates the initiatives' goal or objective/s, the targeted group and the topics included on training programmes.

Table 2: Cyber Security Awareness Initiatives in South Africa

SA CSA Initiatives	Goal /Objective/s	Targeted Audience	Topics Discussed
CSIR (DPSS-CCIW)	To educate current and future users of the computers on safe and secure online habits To increase awareness and understanding of the dangers of the Internet To provide individuals with the necessary knowledge to make the right decisions in Internet-related situations	Secondary schools, Further Education Training colleges Technical university students Non-technical university students Community centers Support staff Educators/Teachers	Physical Security, Malware and countermeasures, Surfing, Social aspects of cyber security

UP ICSA-PumaScope	Falls under an existing project is called PumaScope, and is the main focus of UP's cyber security awareness initiatives	Rural schools (children and adults), churches, orphan homes	Topic varies as it is community based project
UNMM (ISM)	To educate the users about information security or, more specifically, to educate users about the individual roles they play in the effectiveness of one type of control, namely, operational controls.	General company end-users, entrepreneurs (public or private sectors), children, parents, tertiary and senior citizens.	Passwords management, information security principles and terminology, social engineering, phishing, desktop security, patch management, updating anti-virus software and backup procedures, email security,
UNISA	To contribute towards the creation of cyber awareness culture.	School children	Cyber security concepts
UFH	To improve performance in the areas in which an organisation has identified performance deficiencies. To test students' personal information security competency level because a user can be aware of an issue but not necessarily act on the knowledge that the person has gained.	University students (1st and 3rd year-levels)	Passwords management, information security principles and terminology, social engineering, phishing, desktop security, patch management, updating anti-virus software and backup procedures, email security,
SABRIC	To deliver measurable value to our clients through a team of energetic specialists who consistently provide high quality support services and products and, To contribute to the reduction of bank related crime through effective public private partnerships.	South African Banks' (SABRIC partners) Employees	Commercial fraud, online scams, device scams, online safety practise
ISG Africa	To drive awareness and education around information security risk and governance.	Organisations and society	Cyber threats and information security
South African Centre for Information Security (CIS)	To develop and promote a management and governance drive to implement effective information security programs	Organisations in all aspects	Cyber crime

Table 3 illustrates the initiatives as well as their corresponding collaborations and their locations, the methods used by the initiatives to interact with target groups, the methods used to evaluate the programme and the outputs. Some of the organizations who provide such initiatives include:

Council for Scientific Industrial Research (CSIR) and University of Venda: The CSIR and the University of Venda are collaborating to raise cyber security awareness in local rural communities in the South African Limpopo province, Vhembe district. The motivation behind this initiative is to prevent innocent Internet users from becoming victims of cyber attacks, by educating novice Internet and technology users with regard to basic security (Grobler 2011).

University of Pretoria (UP) (ICSA- PumaScope): UP embarks on numerous community-based projects that serve many geographical areas in South Africa. An existing project is called PumaScope, and is the main focus of UP's cyber security initiatives awareness initiatives. It focuses on the transfer of knowledge in the areas of Computer Science, including basic computer literacy and cyber awareness (Grobler 2011).

Table 3: Cyber Security Awareness Initiatives in South Africa

SA CSA Initiatives	Collaboration/ Location	Delivery Methods	Evaluation Methods	Output
CSIR (DPSS-CCIW)	Univen, SAFIPA, Meraka, UP, Mpumalanga/ Pretoria	Presentation, Board and computer based games, Movie clips	Pre- and Post-Survey	Reports, Publication
UP ICSA-PumaScope	Mpumalanga, Gauteng, Microsoft, Atos origin/ Pretoria	Presentations	Surveys	Accredited certificates by the Department of Computer Science at the University of Pretoria.
UNMM (ISM)	Not mentioned/ Port Elizabeth	Computer Science portal, short learning Program, Module e-learning, competitions, gamming education	Survey	Degrees, paper publications, technical projects, games and content specific sites
UNISA	Not mentioned/ Pretoria	Schools' curriculum preparations and research	N/A	Curriculum, degrees and paper publication
UFH	Not mentioned/ East London	Formal lecture	Online questionnaires	lecture, textbook chapters and notes, Paper publication
SABRIC	Most South African banks/ Gauteng	Online discussion, web-portal and formal presentations	N/A	Reports
ISG Africa	Business against crime and SABRIC, South Africa and Africa/ South Africa	Web-portal and online discussions	N/A	N/A
South African Centre for Information Security (CIS)	Not mentioned/ South AfricaS	Discussions and presentations	N/A	Reports

University of Nelson Mandela Metropolitan (UNMM) (ISM): The Information Security Management research group at NMMU has been involved in research in the area of cyber security for more than a decade. The focus of the research group addresses all aspects of information security management, with information security awareness and related areas receiving a lot of attention. Many papers have been published and presented in these fields of information or cyber security awareness, culture and education (Grobler 2011).

University of Fort Hare (UFH): The Information Systems group at UFH conducted a study amongst a group of the university student within the campus who were non-IT. The focus of the group is to increase its capability in terms of keeping the computer users within the university aware of the threats and vulnerabilities that comes with the use of computers and Internet (Grobler, 2011).

University of South Africa (UNISA): The Information Security Awareness research group at UNISA works on a project that is mainly for children, adults and elderly. The initiative aims at teaching these groups on self responsibilities in securing their computers. (UNISA, 2011).

South African Banking Risk Information Centre (SABRIC): SABRIC was established as a wholly owned subsidiary of the Banking Association and is funded by most of South African banks. The centre has a public awareness initiative that is directly available on its website. the initiative focuses mainly on public needs and teaches public the best practises on the use of banks facilities and general security. It further gives tips on new scams and guidelines to follow if one becomes a victim (SABRIC, (2011).

Information Security Group of Africa (ISG-Africa): ISG-Africa consists of security professionals from corporate, government and IT / legal firms within Africa. The focus of this group is to establish, promote, manage and control various interest and user groups, for the promotion of education, and awareness of information security (ISG-Africa, 2011).

South Africa Centre for Information Security (CIS): CIS was established to develop and promote a management and governance drive to implement effective information security programs. CIS has a section where cyber crime is discussed and explained in details (SA-CIS, 2011).

Analysis of these initiatives shows that universities and research institutes such as the CSIR are at the forefront of the campaign to create cyber security awareness to the communities. There are some business organisations that have been identified but the details of how they conduct security awareness remain confidential. The authors understand that the list presented here is not exhaustive; these that are presented in this paper are those whose activities are on the public domain.

Most of the initiatives meet the basic requirements as all of them have plans, objectives, methods of delivery etc. Fifty percent of the identified initiatives have collaborative partnerships with other organisations and again fifty percent have methods to evaluate the initiative/programme. Furthermore, majority of the initiative make a huge contribution to the body of knowledge as seen by the number of publications, qualifications and reports.

3.1.2 Evaluation of effectiveness of Cyber Security Awareness initiatives in South Africa

Table 4 below illustrates the evaluation of cyber security awareness initiatives against the key factors of cyber security awareness programme specified by Peltier (Peltier, 2005). The key factors includes the analysis of cyber crime, identification of target group, identification of the need of target group, evaluation of plans, evaluation methods and the involvement of the government.

Table 4: Evaluation of CSA initiatives

Initiatives	**Does the initiative give a coherent analysis of the state of cyber crime?**	**Is the target group identified?**	**Are the needs of the identified group understood ?**	**Are the plans implementable ?**	**Are there Measures of Effectiveness ?**	**Is the governme nt involved?**
CSIR (DPSS-CCIW)	Yes	Yes	Yes	Yes	Yes	No
UP (ICSA-PumaScope)	Yes	Yes	Yes	Yes	Not Specified	No
UNMM (ISM)	Yes	Yes	Yes	Yes	Yes	No
UNISA	Yes	Yes	Yes	Yes	Not Specified	No
UFH	Yes	Yes	Yes	Yes	Yes	No
SABRIC	Yes	Yes	Yes	Partially	Not Specified	No
ISG Africa	Yes	Not Specified	Not Mentioned	Partially	Not Specified	No

South African Centre for Information Security (CIS)	Yes	Not Specified	Not Mentioned	Partially	Not Specified	No

From Table 4, it is evident that all the initiatives identified address all the key issues of cyber security awareness with the exception of government involvement and measures of effectiveness. The limited or absence role of the government in these initiatives remains a huge concern and this together with the lack measures of effectiveness in most initiatives may hamper the roll out of cyber security awareness to wider communities.

4 Conclusion and Future Work

This paper presented some of the cyber security awareness initiatives in South Africa. These were analysed in terms of their target group, topics covered, collaboration, delivery methods, evaluation measures and the expected output. The initiatives were also evaluated against the key issues that any cyber security awareness initiative must tackle.

Analysis shows that the current initiatives are effective and have been able to address cyber security issues although at a smaller scale. This is despite the fact that South Africa is yet to develop a cyber security policy. Presently, universities are at the forefront with limited participation from the government. The business sector on the other hand seems to be engaging in cyber security awareness activities, though separately. A savvy cyber security aware nation requires that all levels of society be serviced. The initiatives are focusing largely on the communities. Literature material read for this paper indicates that these initiatives are comparable to the international counterparts.

It is therefore recommended that, a single body that will integrate all activities of all cyber security awareness initiatives is needed. It is envisaged that this body will develop a collaborated framework that spreads out all cyber security awareness across the country. Furthermore, this body can set standards procedures and measures for all its members to conform to. This body can also play the regulatory function to ensure that only quality cyber security awareness material is developed and presented to communities.

The formulation of the national cyber security awareness framework will be proposed in future, which will incorporate all the necessary roles and responsibilities of each initiative in order to ensure that the programmes reach all corners of the country.

References

Carnegie Mellon_ CyLab, (2008). *"Message from Mauritius (Part II): Holistic Cyber Security Strategy -- Professional & Personal",* available online from: http://www.gov.mu/portal/sites/csd/downloads/ppt/Track3/Mauritius.pdf, (accessed on 13/03/2011)

Cyberspace Policy Review, (2011). *"Assuring a Trusted and Resilient Information",* [online], http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (accessed on 10/07/2011).

DiGregory, K., (2000). "*Fighting Cybercrime-What are the Challenges Facing Europe?",* Meeting before the European Parliament; United States Department of Justice [online], http://www.justice.gov/criminal/cybercrime/EUremarks.htm, (accessed on 08/01/11).

Dlamini, I.Z Taute, B. and Radebe, J., 2011. *"Framework for an African Policy Towards Creating Cyber Security Awareness"*, [online], http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf, (accessed on 22 /09/2011).

Ferrier International, (2011). "*Business Against Crime South Africa on the Latest Crime Statistics",* [online], http://ferrierinternational.com/business-against-crime-south-africa-on-the-latest-crime-statistics/, (accessed on 05 /03/2011).

Fick, J., (2009). "*Cybercrime in South Africa: Investigating and prosecuting cybercrime and the benefits of public-private partnerships",* Council of Europe octopus interface conference cooperation against cybercrime, pp 10-1, (accessed on 08/07/11)

France 24, (2011). *"Cybercrime costs $114 billion a year: Report",* [online], www.physorg.com/news/2011-09-cybercrime-billion-year.html, accessed on (accessed on 16 /07/2011).

Grobler, M., Flowerday, S., von Solms, R. and Venter, H., (2011). *"Cyber Awareness Initiatives in South Africa: A National Perspective*", [online], http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf(accessed on 19/08/2011).

ISG-Africa, (2011). *"CYBERCRIME: Safety & Security Guide",* [online], http://cybercrime.org.za/local-resources/, (accessed on 25 /09/2011).

IST-Africa, (2011). *"Proceedings of the First IFIP TC9 / TC11-Southern African Cyber Security Awareness Workshop 2011",* [online], http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf, (accessed on 23 /09/2011).

Ministry of Defence-Estonia, 2008. *"Cyber Security Strategy- Cyber Security Strategy Committee",* [online], http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf, (accessed on 27/08/2011).

Ngundi, V. (2010). Cybercrime, Cybersecurity and Privacy, available online from: http://www.eaigf.or.ke/files/2010_KIGF_Cybercrime_Cybersecurity_and_Privacy.pdf, (accessed on 05/03/2011)

Obama, B.H. 2009. Remarks By The President On Securing Our Nation's Cyber Infrastructure, BH Obama, President of the United States of America; The White House, Office of the Press Secretary, [online], http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/, (accessed on 13/03/2011).

Peltier, T., (2005*) "Implementing an Information Security Awareness Program".* Information Systems Security 14. Vol. 2, pp. 37–49.

RSA, (2011). *"Cyber Security Awareness Month Fails to Deter Phishers",* [online], http://www.rsa.com/solutions/consumer_authentication/intelreport/11541_Online_Fraud_report_1011.pdf, (accessed on 22/04/2011).

South African Government Gazette, (2010). *"South African National Cyber Security Policy",* [online], http://www.pmg.org.za/files/docs/100219cyber_security.pdf, (accessed on 02/06/2011). ISSUE?

SABRIC, (2011). *"Public Awareness", [online], https://www.sabric.co.za/?pg=Public+Awareness, (accessed on 02/06/2011).*

South African Centre for Information Security, (2011). *"What is cyber crime",* [online], file:///I:/Attention/ICIW%202012/22%20November%202011/definecrime.htm, (accessed on 16 /09/2011).

South African Police Service, (2011). *"Crime Report 2010/2011: South African Police Service (SAPS)"*, [online], http://www.saps.gov.za/statistics/reports/crimestats/2011/crime_situation_sa.pdf, (accessed on 19/08/2011).

The New Age, (2011). *"SA a target for cyber crime",* [online], http://thenewage.co.za/printstroy.aspx?news_id=28862&mid=53, (accessed on 22/09/2011).

UNISA, (2011). Information Security Awareness research group, [online], http://www.unisa.ac.za/default.html, (accessed on 12/08/2011).

Wolrd Cutoms Organization, (2011). *"Terms of Reference for the Working Group on Commercial Fraud",* [online], http://www.wcoomd.org/home_about_us_committstructcommrfraud.htm, (accessed on 16/07/2011).

Zuma, J.G. (2009). State of the Nation Address by His Excellency, JG Zuma, President of the Republic of South Africa; [online], http://www.parliament.gov.za/content/SONA3June2009.doc, (accessed on 27 /09/2011).