Evaluating Cyber Security Awareness in South Africa

Marthie Grobler[1], Joey Jansen van Vuuren[1] and Jannie Zaaiman[2]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]University of Venda, South Africa
mgrobler1@csir.co.za
jjvvuuren@csir.co.za
jannie.zaaiman@univen.ac.za

Abstract: In many ways, the internet and cyber world is a dangerous place where innocent users can inadvertently fall prey to shrewd cyber criminals. These dangers, combined with a large portion of the South African population that has not had regular and sustained exposure to technology and broadband internet access, expose local communities to cyber threats. Research done by the Council for Scientific and Industrial Research and the University of Venda shows that these local communities are not empowered to deal with these threats. To prevent innocent internet users from becoming victims of cyber attacks, an intensive awareness campaign is planned to educate novice internet and technology users with regard to basic security. The motivation for this awareness project is to educate all South Africans using the internet, in an attempt to strengthen the awareness level concerning the South African network - if there are local communities that are not properly educated, their technology devices may remain unprotected. This may leave the South African internet infrastructure vulnerable to attacks, posing a severe threat to national security. In this specific project, national security will be promoted through awareness training focusing on the newly released broadband capability and knowledge transfer within rural communities. To evaluate the current level of cyber security awareness, a series of exploratory surveys have been distributed to less technologically resourced entities in rural and deep rural communities within South Africa. By analysing the results of the surveys, it is possible to benchmark the current level of awareness. These observations can then be extrapolated to the larger group of rural South African communities. The next stage of the awareness evaluation project is to develop cyber security awareness training modules for the local communities in their native tongue, aimed to improve the current level of awareness. This paper discusses the preparation, evaluation and training of South African rural communities with regard to cyber security awareness. Due to the networked nature of the internet, the level of awareness has an influencing impact on the global community. Thus, to ensure a safely protected South African network, it is necessary to target the communities that can inadvertently leave the network vulnerable.

Keywords: cyber security, awareness, rural communities, broadband, training, South Africa

1. Introduction

Cyber space is a complex environment that can advance individuals' experience of electronic dependent activities, but can also place these individuals and their respective nations in a vulnerable state. Cyber space, cyber awareness and cyber security play an important role in the online experience of individuals, and need to be addressed accordingly. The internet and cyber world is a dangerous place where innocent users can inadvertently fall prey to shrewd cyber criminals. These dangers, combined with a large portion of the South African population that has not had regular and sustained exposure to technology and broadband internet access, expose local communities to cyber threats.

Research done by the Council for Scientific and Industrial Research (CSIR) and the University of Venda shows that these local communities are not empowered to deal with these threats. To prevent innocent internet users from becoming victims of cyber attacks, an intensive awareness campaign is needed to educate novice internet and technology users with regard to basic security. The motivation for this awareness project is to educate all South Africans using the internet, in an attempt to strengthen the awareness level with regard to the South African network - if there are local communities that are not properly educated, their technology devices may remain unprotected. This may leave the South African internet infrastructure vulnerable to attacks, posing a severe threat to national security. In this specific project, national security will be promoted through awareness training focusing on the newly released broadband capability and knowledge transfer within rural communities.

2. The impact of broadband penetration on National Security

With the impending increase in broadband access in South Africa, an average citizen's computer or identity could in future be used (with or without knowledge and consent) as a hub for launching cyber attacks on the rest of the world. The modern definition of national security includes human security, the security of the individual as well as the average citizen (Phahlamohlaka, 2008). Africa as a continent recently had an increase in broadband access from a previous 120 Gbps to 12 Tbps over two years. Although the level of cyber attacks from the continent were very low, it could in future be used as a hub

for launching cyber warfare type attacks on the rest of the world. Research done by the United States' Naval Warfare Command indicates that cyber developments moved the battlefield to the average citizen's home: attackers could take over a new computer within 30 seconds after first connection to the internet (Jansen van Vuuren, Phahlamohlaka & Brazzoli, 2010).

This can have a dramatic impact on National Security. For example, there are some arguments that South Africa's strong ties with China could place the country at high risk of cyber war attacks (Stiennon, 2009). The generic National Security framework proposed by Jansen van Vuuren, Phahlamohlaka and Brazzoli (2010) lists a number of cyber security threats to National Security due to the heightened broadband access. These threats can be categorized as either natural determinants or social determinants.

2.1 Natural determinants

Natural determinants are a causal factor influenced by the specific environment analysed.

- **Geography and resources** contributes largely to the impact of broadband penetration in a specific environment. For example, the shipment of outdated computers to Africa poses a security threat since outdated software is vulnerable to attacks due to unavailability of updates. Taken into consideration the 100 million computers in Africa the access will result in internet users and especially individuals in rural communities being attacked regularly.
- The **population** in a specific environment provides the extent to which broadband penetration can have an impact – the bigger the population, the higher the potential broadband penetration. For example, the occurrence of botnets may drastically increase if internet connectivity is higher, as with high broadband access. This will result in armies of networked compromised computers in the homes of many South Africans, posing serious threats to a country's National Security.

2.2 Social determinants

Social determinants are a causal factor influenced by the groups and individuals in the specific environment analysed.

- The **economy** plays a motivator role in the impact of cyber threats. Recently South Africans experienced several extensive scamming attacks, of which the most prominent the herding of personal information using South Africa Revenue Service (SARS) and the fraudulent World Cup offers supposedly from South African Airlines (SAA). Many people have already succumbed to these fraudulent emails that gather their personal information. South African banks are also currently experiencing an increase in banking fraud that directly poses a threat to individuals that may lose their savings.
- **Politics** has a direct influence on National Security. Accordingly, attacks on websites of the African National Congress (ANC) - the ruling party in South Africa - with the aim of discrediting the party, or the use of party member names to scam money from innocent citizens, resulted in embarrassment to the party and a tumultuous political environment. A fraudulent email discussing a national strike in the near future created uncertainty and could have created instability in the country.
- The **military** is responsible for protecting a country's National Security. Currently, many South African citizens are not security savvy enough to thwart cyber attacks successfully, potentially leaving the South African network compromised and open for attacks on a larger national scale.
- **Psychology** can play a large role in the social aspects of cyber threats. For example, Distributed Denial of Service (DDoS) attacks were already used to compromise websites and place Psychological Operations (PsyOps) messages on compromised websites, as seen in the Georgia attack in 2008. Recently, cell phones were also used to organise protests and influence citizens to take part in a national strike that paralyzed Mozambique's capital (AFP, 2010).
- **Information** is paramount in any cyber threat. South Africa identified the need for Information Communication and Technology (ICT) access to all its citizens that must be promoted on all levels of the community and everybody must be exposed to the use and benefits of ICT. Along with increased broadband access and connectivity by all its citizens, there are the possibilities of viruses that could damage user's computers and information. Malicious code can also be used to overwrite the infected computer's hard drive which could result in massive loss of data and information as experienced in Korea with the DDoS attacks (Kebbs, 2009).

The results of this analysis indicated the necessity of security awareness in South Africa to combat these cyber threats. Since both natural and social determinants are commonplace and both these determinants potentially have a major effect on a country's information infrastructure, it is necessary to consider the broadband penetration when planning a cyber security awareness project.

2.3 Governments' responsibility

In the light of existing international law doctrine a country may be considered responsible for acts performed by residents if the country explicitly authorised these acts on its behalf. The country may also be held responsible for a breach of an international obligation, or for not preventing an attack from taking place (Kulesza, 2010). Developments in global technology make it difficult for a country to control its residents' actions in operating hardware located within the country's territory, and nearly impossible to control non-residents outside a country's jurisdiction that controls hardware inside the country's jurisdiction. Regardless of the associated difficulties, cyber crime is a reality that unfortunately often targets the uneducated individuals that do not know how to identify cyber scams or how to keep their computers protected.

Therefore, South Africa can be considered responsible for preventing attacks from inside its borders to other countries. It is accordingly the responsibility of the South African Government to support extensive awareness programs to prevent attacks from inside South Africa's borders on other countries. In its quest to manage Cyber Security, a formal notice was issued in February 2010 regarding its intention of publishing a South African National Cyber Security Policy (Gazette No 32963, Feb 19, 2010). The country did this within the context of its global citizenry and the commitment it has made to the World Summit on Information Society (WSIS) in 2001, and to the International Telecommunication Union (ITU) to assist in further development of the Global Cyber Security Agenda (GCA). One of the elements of this policy is the importance of cyber security awareness programs for South Africa.

3. Situational analysis – the case of the Vhembe district

The CSIR and the University of Venda's schools of Mathematical and Natural Sciences, and Management Sciences are collaborating to raise cyber security awareness in local rural communities in the South African Limpopo province, Vhembe district. In Phase 1, a group of CSIR researchers trained a number of student volunteers at the University of Venda to teach specific groups of computer users, including secondary school users, further education training users, university (non-technical) users and community centre users. More rural communities are becoming integrated into the global village due to increased hardware and software corporate donations, the proliferation of mobile Internet devices and government programmes aimed at bridging the digital divide. The next section will provide some information on the area.

3.1 Limpopo Province

The Limpopo Province comprises four districts: Vhembe, Capricorn, Greater Sekhukhune Waterberg and Mopani. In 2001, 33% of the population aged 20 years or older in Limpopo had no education at all, while 7% had post-high-school education (see Table 1). These figures, in general, show an increase in all categories since 1996 with the exception of the *no schooling* category. This decrease indicates a higher percentage of people attending school.

Table 1: Level of education among adults 20 years or older, in Limpopo, 2001

	Number	**%**
No schooling	789731	33
Some primary education	336377	14
Completed primary education	133206	6
Some secondary education	629057	26
Grade 12/Standard 10	337627	14
Higher education	162454	7
Total	**2388452**	**100**

In Limpopo there are approximately 4290 primary schools and 1300 secondary schools with over 1.8 million learners and almost 58000 teachers (2002). In 2002 less than 10% of the schools in the province were computerised and fewer than half of those were really utilising their computers. Since then the

situation has improved, mainly due to a considerable amount of donations, but many schools still lack computers, connections and capabilities related to them.

In higher education institutions in Limpopo, there are about 40000 students enrolled per year. The number of university graduates is about 15000 per year, with only 4% graduating in ICT related fields. The Limpopo province had an enrolment figure of 10500 for 2010.

3.2 Vhembe District

The Vhembe District covers 21407 square km of land. It was originally settled by tribes of Khoisan people. It was later settled by the Venda people (recently migrated from what is now Matabeleland South in Zimbabwe), who constitute a majority of the Vhembe population today. According to the DWAF Stats Form-D study, the Vhembe population has increased and is now standing at 1.388427 million people. The number of households is estimated at 269547, with 50% of the population being under the age of 20 years. The District is still faced with infrastructural backlog, with 53% of the population not having access to running water, 68% of the population not having access to sanitation, and 46% of the population not having access to basic levels of electricity (Vhembe District Municipality, 2007). As a result, much of the population would use centralised community centres or internet cafes to access the internet.

About 57% of the population does not have formal education, 9% has primary education, 20% has secondary education and only 3% has tertiary education. The main contributions to the economy are community services (22%), trade (14%) and mining (0.7%). Tourism, agriculture and manufacturing are also significant with potential to be further enhanced. The unemployment level is at 53% (Vhembe District Municipality, 2007). Tables 2 to 5, and Figure 1 show a range of demographic related statistics on the population of the Vhembe District.

Table 2: Local municipalities (Vhembe District Municipality, 2007)

Local municipality	Population	%
Thulamela	584 568	48.72%
Makhado	497 093	41.43%
Mutale	78 917	6.58%
Musina	39 308	3.28%

Table 3: Language and population demographics (Vhembe District Municipality, 2007)

Language	Population	%
Venda	818 900	68.25%
Tsonga	316 703	26.40%
Northern Sotho	27 922	2.33%
Afrikaans	13 697	1.14%
Sotho	7 714	0.64%
Other	5 942	0.50%
English	4 545	0.38%
Ndebele	1 763	0.15%
Zulu	870	0.07%
Tswana	840	0.07%
Xhosa	659	0.05%
Swati	331	0.03%

Table 4: Gender composition (Vhembe District Municipality, 2007)

Gender	Population	%
Female	662 815	55.24%
Male	537 041	44.76%

Table 5: Ethnic groups (Vhembe District Municipality, 2007)

Ethnic group	Population	%
Black African	1 181 672	98.48%
White	13 625	1.14%
Indian/Asian	2 911	0.24%
Coloured	1 648	0.14%

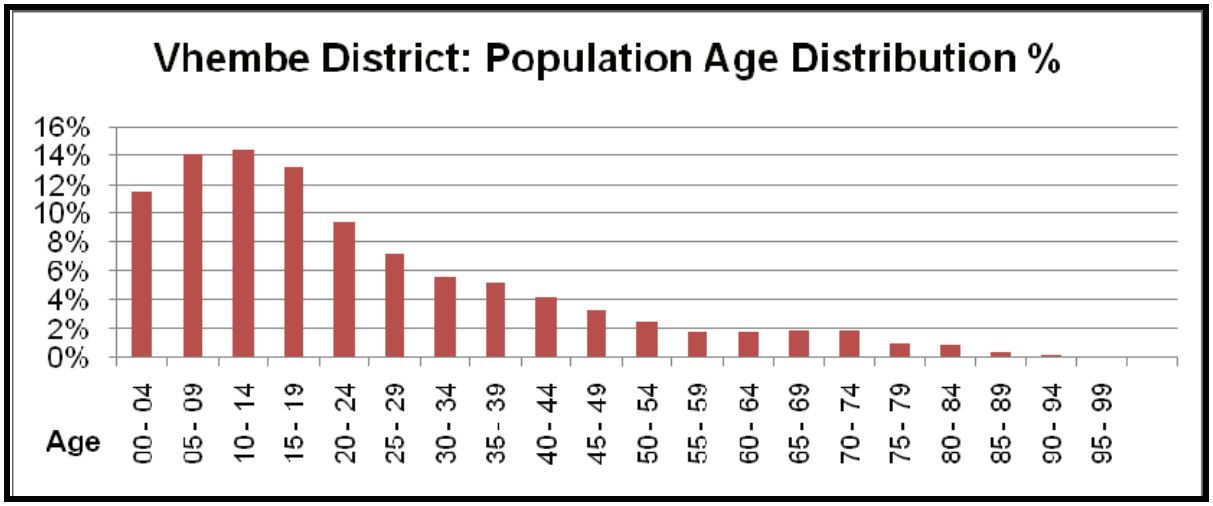

Figure 1: Age analysis (Vhembe District Municipality, 2007)

These new netizens in rural communities are not cyber security savvy. This is why cyber security self-defence workshops for volunteer facilitators in the Vhembe district were introduced. Discussions for the initiative started at the end of 2009 but the formal planning, collaboration and the development of the cyber security awareness training programme officially commenced in May 2010.

4. Current level of awareness in the Vhembe district

The proposed cyber security awareness training module is part of a larger project that aims to establish an Institute for Broadband and Rural ICT Development at the University of Venda to assist rural communities in adapting to the opportunities presented by broadband and other forms of ICT. As part of the project, the CSIR developed surveys to assess the current level of cyber security awareness within the communities. Large numbers of these surveys were distributed to some of the community centres and schools participating in the project.

During the second part of 2010, a number of surveys were distributed to both educators and secondary school learners in the Vhembe District. These surveys were presented to participants before any cyber security awareness training material was presented to them, intended to test current awareness of cyber related topics. The surveys were presented in English, which is not the mother tongue for most of the participants. The results presented next accordingly need to take potentially language barriers into consideration.

4.1 Educators' survey

One of the initial pilot studies was done with educators attending a community centre focused on the development of Mathematics and Science of learners in rural communities. Participants in the survey indicated that they do not have a problem with English as spoken language, but they are not comfortable with English as a written language. These results were confirmed with contradicting answers given in the surveys. Participants were mostly over the age of 30 and thus did not grow up in the technological era for these rural communities. More than 90% of the participants have cell phones, but they indicated that this is used mostly for text messaging and verbal communication.

Although 67% of the participants have access to a computer (either at home or at work), the participants indicated that they do not make use of computer-based instant messaging. Participants with access to computers do make use of the internet for informational purposes. Participants indicated that the use of the internet for e-commerce was limited and that they prefer not to make use, for example, of the South African online system for income tax completion (e-filing). Most of the participants correctly indicated the

meaning of *social networking*, whilst only 44% knew what the terms *phishing* and *viruses* meant. Participants did not know what a strong password is but did indicate that they will not reveal their passwords to one another. Participants indicated that they would advise their children to meet online friends in places other than chatting rooms. This can potentially place the children in danger of meeting sexual predators in a real world scenario. A further concern is that 44% of the participants were prepared to submit their personal details to a popular website, with no regard of the security implications and potential for identity theft. Although the sample group did not constitute a large percentage of the educator group in the Vhembe District, the results clearly indicate that the current cyber security awareness level is relatively low, and there is a dire need for urgent awareness training. This pilot study therefore serves as additional motivation to continue the research and roll out the awareness training on a larger scale within the Vhembe District.

4.2 Secondary schools' survey

Surveys were distributed at two secondary schools in the Vhembe District. At School A, 69% of participants indicated that they were comfortable with English as a written language, whilst 15% indicated that they were only comfortable with English as a spoken language. At School B, 26% of participants indicated that they were comfortable with English as a written language, whilst 84% indicated that they were only comfortable with English as a spoken language. At both schools, majority of participants indicated that they only have access to cell phones as technology devices. At both schools, only 7% of participants have had prior access to a desktop computer. Participants with access to computers or cell phones connected to the internet use it for entertainment and gaming.

At both schools, most of the participants correctly indicated the meaning of *phishing* and *social networking*. Although not all participants have regular access to social networking sites or online chatting, they are aware of some of the inherent dangers of communicating over the internet. Most participants indicated that they would not arrange an actual meeting with someone that they have met online. 99% of all participants have indicated that they will not submit personal information on a website, even if that website is very popular. At School A, 69% of participants indicated that it is wrong to break into someone else's email account and send emails pretending to be the other person. 23% of participants indicated that they would like to learn how to break into someone else's email account. At School B, only 24% of participants indicated that it is wrong to break into someone else's email account and send emails pretending to be the other person, whilst 100% of participants indicated that they would like to learn how to do this. Most participants correctly identified weak passwords. Typical to the general classification of Millennials or Generation Y (individuals born between 1982 and 2000), the participants show increased tendencies towards ambition, new challenges and inquisitiveness (Kane, 2010). The participants have created a long list of topics that they would like to see addressed in future cyber security awareness training programs.

4.3 Development of training material

The proposed cyber security awareness program focuses on educating beginner internet and technology users in basic computer security, and safe and secure online habits. The objective of this program is to prepare civilians for use of broadband applications and new applications for cyberspace. It aims to increase awareness and understanding of the dangers of the internet, whilst providing individuals with the necessary knowledge to make the right decisions in internet-related situations. This program is not a computer literacy course, but can be better defined as a self-defence course for internet users. The target audience is computer users with working computer literacy and awareness and prior exposure to the internet. These individuals should not have any formal computer related training, with the exception of computer literacy courses. For the time being, four user groups are identified:

- Secondary school pupils,
- Further education training (FET) college students,
- University students not studying towards a technical or information technology degree, and
- Community members using the computer facilities of community centres.

The program is rolled-out in the Vhembe District, Thohoyandou in the Limpopo province of South Africa. Within the province, entities had to be selected to partake in this program. Two classifications are used for entity selection, as shown in Table 6.

Table 6: Classification regarding entity selection

	Less resourced entity	More resourced entity
Internet connection	1 modem	> 1 modem or ADSL
Number of computers	< 5	5 or more
Number of users/computers	100:1	99:1 <
Level of maintenance (functionality)	Less than 50% working	More than 50% working

For the initial training program, only schools and centres that have previous exposure to computer facilities and internet access are selected as participants in the setup.

The cyber security awareness program modules are divided into four main topics:

- Physical security – This training session addresses the importance of securing the physical computer in order to protect the computer user from potential cyber security dangers. This session addresses the physical protection of computers, laptops and mobile phones, as well as the importance of password protection.
- Malware and malware countermeasures – This training session touches on some of the different types of malware that can be encountered in cyberspace, and provide guidelines on how to protect a computer or mobile phone from these malware types.
- Safe surfing – This session addresses the guidelines that internet users should practice to ensure that the time they spend online are productive and secure. This session addresses internet surfing, email security, file sharing, copyright, downloads and storing in more detail.
- Social aspects of cyber security – This session addresses the safest way to use social networking, as well as the dangers that are associated with social media on the internet and cyberspace. This session also introduces social engineering, identity theft, cookies and cyberbullies.

5. Feedback from student trainers

In September 2010, researchers from the CSIR have trained a number of volunteers from the University of Venda to train the community. The majority of these students are second and third year computer science students from the University of Venda. These students assisted with the distributions and collection of initial surveys to the participating entities to determine the current level of cyber security awareness. After completing the training, the student trainers completed questionnaires about their experience. Figures 2 to 5 show the student trainers' feedback on the content of the training modules. Since the number of trainers needed for the pilot project was relatively small, the responses to the questionnaire are not indicative of the awareness level of the intended target audiences, but rather an indication towards the usability of the training modules.

From Figures 2 to 5, it is clear to the student trainers found the training modules very useful and informative. Where necessary (e.g. community centre, topic cookies), the material were adjusted according to the feedback received from the student trainers.

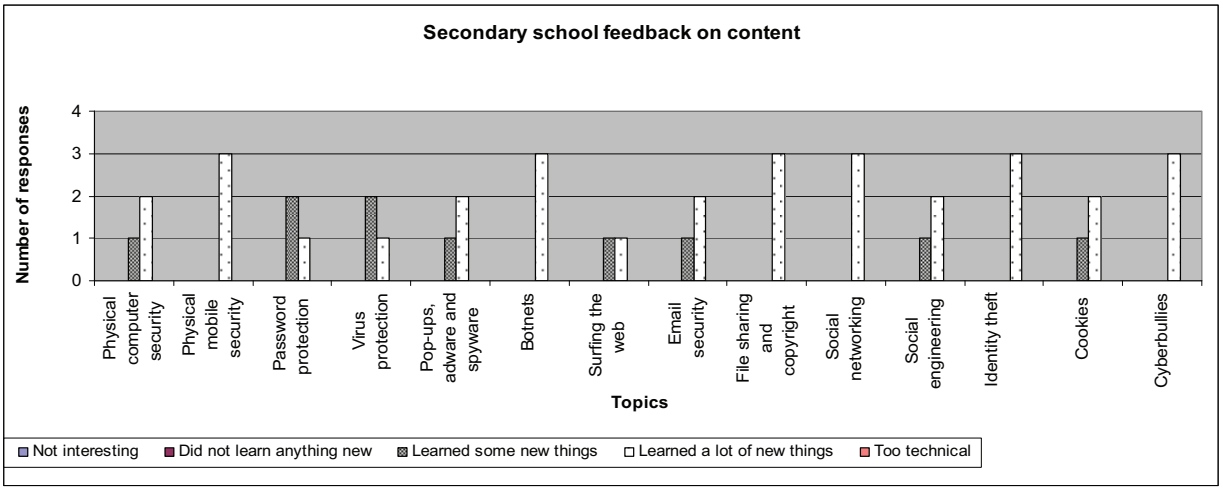

Figure 2: Feedback on the content of the secondary school training module

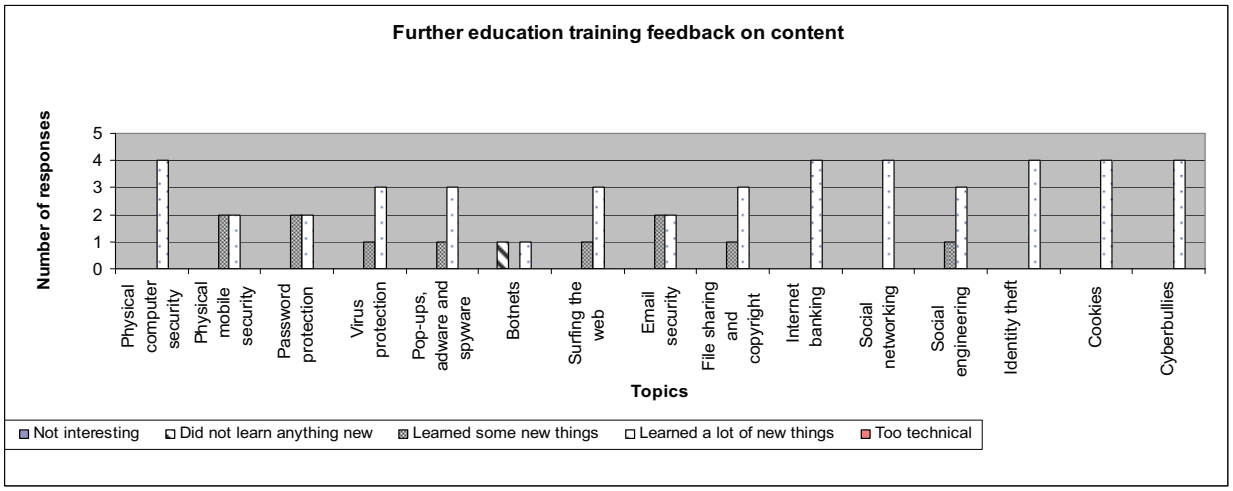

Figure 3: Feedback on the content of the FET training module

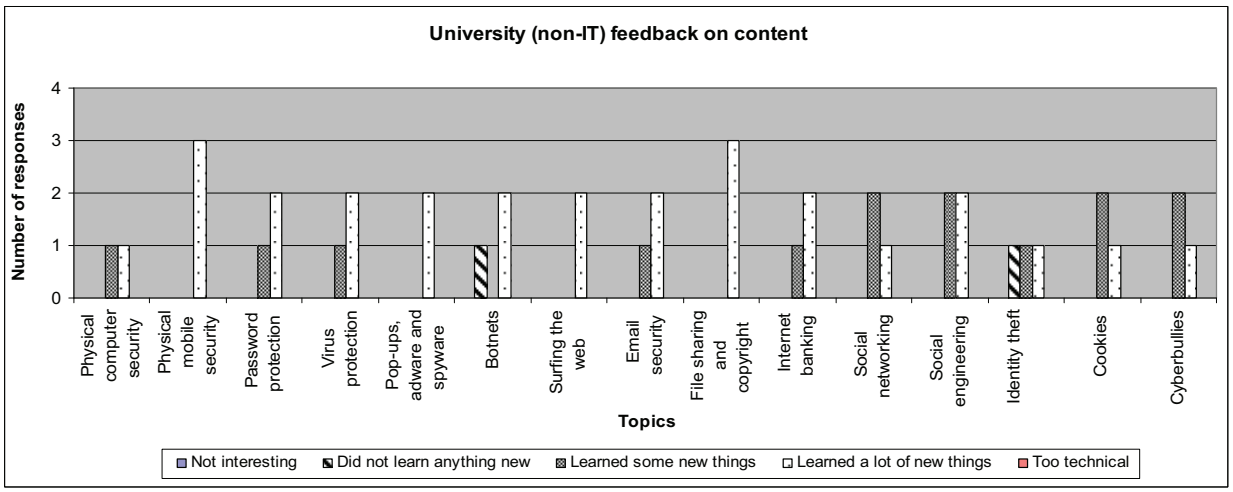

Figure 4: Feedback on the content of the university training module

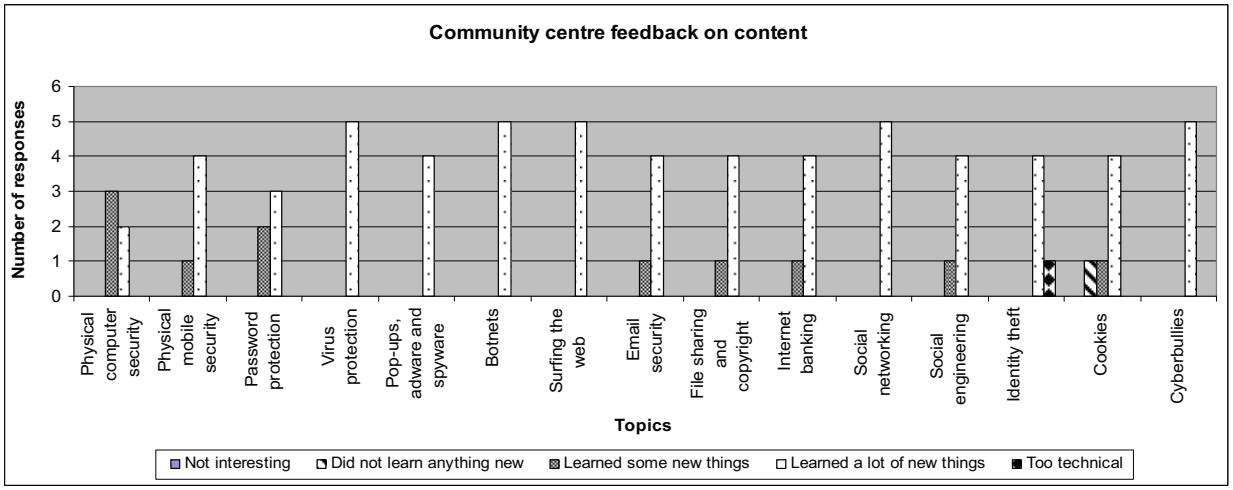

Figure 5: Feedback on the content of the community centre training module

6. The way forward

The next step in the cyber security awareness program is to roll the training material out to the community. Each of the students that were trained is allocated to a specific entity. These students have to train the community in their specific entity. The community training program is free of charge, but the volunteers need to adhere to specific conditions in order to participate in the program:

- The volunteer needs to complete a questionnaire before starting the training. This questionnaire will not be anonymous and will allow the CSIR to score the individual's current level of cyber security awareness.
- The volunteer needs to be willing to attend classes organised and hosted by the student volunteer trainers from the University of Venda. The trainers will communicate the dates and times of these training with the volunteers. To be a part of this training, the volunteer needs to attend all the classes and workshops.
- The volunteer needs to complete a questionnaire after completing the training. This questionnaire will not be anonymous and will allow the CSIR to score the individual's awareness after completing the program.

The questionnaires consist of three sections. *Basic demographic information* is asked in order to customize the cyber security awareness training program to fit a specific user group and in order to identify an individual's level of awareness. *History and background – Technology* questions are asked in order to determine the current level of technology usage within the specific user's environment. *Specific scenarios* are asked to determine the current level of cyber security awareness and understanding within the specific user's environment.

7. Conclusion

The results from the pilot surveys hint toward a low level of awareness regarding the implications and dangers of cyber warfare and the consequences of participation in social networks. Although the current research is based on an exploratory study with a small group of participants, the research uncovered a need for intensive further training in a number of identified modules, including secondary schools, further education training colleges and community centres, as well as all university staff and students. The main benefit of a large scale roll out of this cyber security awareness training programme is that empowered trainees should be able to identify the dangers of providing information and/or enrolling on social networks where they and their personal information can be exposed and the information could be abused. Further awareness training targeted at the different stakeholder groupings should ensure that capacity is build and that the Vhembe District will become one of the first districts in South Africa with a full understanding and appreciation of cyber security and social networking dangers. Further research and additional work toward this project should drastically improve the level of cyber security awareness in South Africa.

References

AFP. (2010). *Mozambique unrest shows power of the SMS*. Available from: http://www.mg.co.za/article/ 2010-09-07-mozambique-unrest-shows-power-of-the-sms (Accessed 15 October 2010).

Jansen van Vuuren JC, Phahlamohlaka. J, & Brazzoli M. (2010). *The impact of the increase in broadband access on National Security and the average citizen.* Journal of Information Warfare. Vol 9(3). Dec 2010

Kane, S. (2010). *Generation Y.* Available from: http://legalcareers.about.com/od/practicetips/a/ GenerationY.htm (Accessed 7 January 2011).

Kebbs, B. (2009). *PCs used in Korean DDoS attacks may self destruct*. Available from: http://voices.washingtonpost.com/securityfix/2009/07/pcs_used_in_korean_ddos_attack.html (Accessed 4 September 2009).

Kulesza, J. (2010). *State responsibility for acts of cyber-terrorism.* Paper presented at the 5th GigaNet Symposium. Available from: http://api.ning.com/files/6Uhv8JceS2kZGH4RRbdEOAwdiHrryXnRiwQO v1MGYU6hEcBG9M4F5irLoK8B56a8hO*0kQ*CbTExGBpq8wjcPQZzChrSUrXV/KULESKA.pdf (Accessed 17 November 2010).

Phahlamohlaka, J. (2008). Globalisation and national security issues for the state: Implications for national ICT policies. *Social Dimensions Of Information And Communication Technology Policy.* Vol. 282/2008 Springer Boston pp. 95-107.

Stiennon, R. (2009). *SA could face cyber war.* Available from: http://ww2.itweb.co.za/sections/ internet/2009/0905291159.asp?A=COV&S=Cover&T=Section&O=C (Accessed 29 May 2009).

Vhembe District Municipality. (2007). *Quality in Service.* Available from: http://www.vhembe.gov.za/docs/ Approved%20IDP%20final%20version%201%202007-8%20-2011-12.pdf (Accessed 2 February 2011).

Wikipedia. (2010). *Vhembe District Municipality*. Available from: http://en.wikipedia.org/wiki/ Vhembe_ District_Municipality (Accessed 2 February 2011).