Cyber Awareness Initiatives in South Africa: A National Perspective

M Grobler[1], S Flowerday[2], R von Solms[3] and H Venter[4]

[1] Council for Scientific and Industrial Research, Pretoria, South Africa

[2] University of Fort Hare, East London, South Africa

[3] Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

[4] University of Pretoria, Pretoria, South Africa

mgrobler1@csir.co.za

sflowerday@ufh.ac.za

Rossouw.VonSolms@nmmu.ac.za

hventer@cs.up.ac.za

Abstract: Cyber space, cyber awareness and cyber security play an important role in the online experience of individuals, and need to be addressed accordingly. The paper looks at some of the current cyber security awareness initiatives in South Africa, the respective scopes and methodologies of the projects, target audience and geographical areas, and interesting statistics pertaining to the specific projects. Some of the projects included in this paper are run by the Council for Scientific and Industrial Research, the University of Fort Hare, Nelson Mandela Metropolitan University, and the University of Pretoria. Current initiatives cover secondary school pupils, tertiary level students, public and private sector enterprises, and senior citizens. The initiatives address general cyber security aspects, as well as more advanced topics such as social engineering and identity theft.

The paper concludes by building on some of the success stories to map out a practical plan for the way forward to enforce better cyber security awareness for South African citizens. Although not exclusive, this paper provides an indication of the communities in need of cyber security initiatives in South Africa, as well as the cyber security components and topics identified as part of individual projects that need to be addressed on a national level. This paper aims to show that synergy between different South African entities can contribute to a working cyber security awareness concept that can be easily adapted to be used by countries in Africa in the area of cyber security awareness.

Keywords: cyber security, awareness initiatives, 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 in a vulnerable state. It facilitates online communication, electronic capability development and information sharing. For the average person,

cyber space is a means to communicate, connect on social networking sites, perform financial transactions, search for information, and a platform for entertainment. For those that do not specialise in cyber security, cyber space poses inherent dangers that can literally rob cyber space users from both their identity and their money. Cyber space, cyber awareness and cyber security play an important role in the online experience of individuals, and need to be addressed accordingly.

This paper looks at the need for cyber security initiatives. It also looks at some of the current national cyber security awareness initiatives in South Africa, as conducted by the Council for Scientific and Industrial Research (CSIR), the University of Fort Hare (UFH), Nelson Mandela Metropolitan University (NMMU) and the University of Pretoria (UP). Current initiatives cover secondary school pupils, tertiary level students, public and private sector enterprises, and senior citizens. The paper then discusses the future of cyber security awareness in South Africa after which the paper concludes.

2. The need for cyber security initiatives

The South African Banking Risk Information Centre has expressed concern about the increase in local phishing attacks [5], the South African Revenue Service has warned many times against online scams [6], and recently, Symantec has urged cricket World Cup supporters to be vigilant of scams that use the sporting event as a cyber hook [7]. Daily international news events emphasise the need for addressing and maintaining a better level of cyber security awareness globally. In addition, both formal and informal research done by the institutes involved indicates that the South African communities are not empowered to deal with cyber threats. As such, it is crucial that security initiatives are undertaken to educate cyber space users.

3. Cyber awareness initiatives coordinated by the CSIR

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.

3.1 Scope and methodology

The project is part of a larger project aimed at establishing an Institute for Broadband and Rural ICT Development to assist rural communities in adapting to the opportunities presented by forms of technology. Currently, four main computer user groups are targeted: secondary schools, further education training colleges, university (non-technical) and community centre users. The CSIR has developed a pre-assessment, a training module (consisting of training sessions, role-playing, workshops, games and multimedia supplements) and a post-assessment per user group. Students from the University of Venda are trained to present this material (where necessary, in native TshiVenda) and to administer the assessments. Thereafter, CSIR researchers analyse the assessments.

3.2 Target audience

The 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 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. The program is rolled-out in the Vhembe District, Thohoyandou in the Limpopo province of South Africa.

3.3 Findings and challenges pertaining to the project

During the pilot project phase in 2010, a number of surveys were distributed to participants. The surveys were presented in English, which is not the mother tongue for most of the participants. Unfortunately, much of the data analysis is skewed due to an obvious language barrier. Since the inception of the cyber security awareness project, more than 120 people in the Vhembe district have been trained. An additional 24 University of Venda students have been trained as volunteer trainers.

At participating schools, most of the participants indicated that they would not arrange an actual meeting with someone that they have met online. However, community centre 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 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.

3.4 The way forward

The results from the pilot surveys indicated the low level of awareness regarding the implications and dangers of cyber warfare and the consequences of participation in social networks. The research also indicated the dire need for intensive further training. Further awareness training targeted at the different stakeholder groupings ensures that capacity is built 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. 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.

The next step in the cyber security awareness program is to roll the existing training material out to larger groups of the Vhembe community. In addition, four further computer user groups are identified and the development of specific modules is underway. Further initiatives include an

interactive wiki as communication medium between project members, volunteers and trainees; translation of all modules into at least four of the South African national languages; and the production of prototype board games and online games to enhance the learning experience.

4. Cyber awareness initiatives coordinated by UFH

An information security competency test was conducted with Bachelor of Commerce undergraduate students at the university in the Eastern Cape during 2010. The purpose of the study was to test students' personal information security competency level. The reasoning behind the project is that a person can be aware of an issue but not necessarily act on the knowledge that the person has gained. Therefore, this survey was conducted in order to understand how many students act on, and implement, what they have been taught with regard to information security.

4.1 Scope and methodology

The research instrument used was an online questionnaire that consisted of nineteen questions measuring both awareness and competency. The questions required respondents to evaluate themselves using a four point Likert Scale or to choose the correct answer (one of five). Human resource practitioners have used competency testing for many years to test the proficiency level of a person in a particular skill area. Additionally, universities often test students to ensure that the student has mastered the course material. The aim of a competency test is to improve performance in the areas in which an organisation has identified performance deficiencies [3] [4]. The initial study involved 50 1st year students and 50 3rd year students.

4.2 Findings pertaining to the specific project

The findings indicate that many 1st year students have a limited knowledge of information security principles and terminology. This was shown in both the awareness questions and the competency questions. Furthermore, the findings indicate that 3rd year students are quite familiar with information security principles and terminology. However, they too scored unacceptably low on the competency questions as many of them have not acted on the knowledge gained during their undergraduate degree.

The 1st year students performed particularly badly in the questions relating to social engineering - only 28% correctly identified the social engineering definition. The social engineering competency testing questions showed that only 12% were competent in understanding what social engineering is. Conversely, 84% of 3rd year students chose the correct social engineering definition, thus one could reasonably assume that upon exiting their degree these students would have been prepared for the workplace. However, the results of the competency testing questions showed only 28% of the students were successful in answering all three phishing questions correctly when identifying social engineering techniques. Figure 1 shows an example of a competency-based phishing question.

The password management results were lower than expected. Although many students correctly identified the definition, many did not demonstrate a clear understanding of how to manage their passwords. Many students indicated that they never change their passwords once set up. Other questions in the survey regarded desktop security, patch management, updating anti-virus

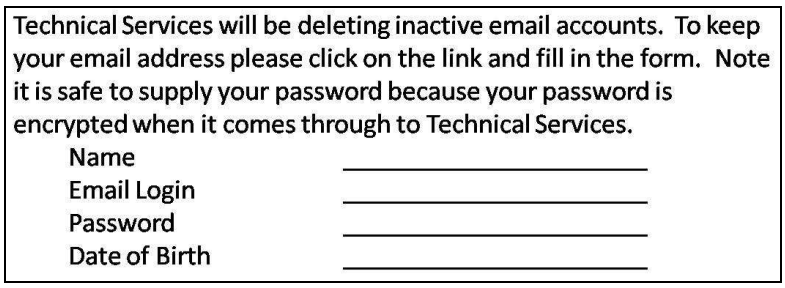

Figure 1: Example phishing question

software and backup procedures. There were also several questions relating to email security. The researchers concluded that even though 3rd year students are aware of many more information security principles and are knowledgeable when it comes to understanding the terminology, there is a degree of apathy and this affects their actions with regard to the implementation of computer security controls.

4.5 The way forward

The first phase of this research project was rather small as it only involved 100 respondents. This has led the researchers to include more questions in the questionnaire and to increase the number of respondents for a much larger scale 2011 implementation. One of the primary reasons to continue with this project is that these initial findings would suggest that an effective awareness programme would need more than posters on the walls and pop-up windows displaying the organisation's security policy when an individual logs onto a machine. In addition, further research will be done into the reasons for the low score of 3rd year students on the competency questions.

These students have a lecturer covering this subject with a PowerPoint presentation, several textbook chapters and additional notes. It appears that this may be academically acceptable as this is the current practice. Nevertheless, perhaps more hands-on practical sessions are required and more enforceable controls by the university's technical support services, for example locking someone out of the network if their password has not been changed regularly or if it is insufficiently strong. This could help the students develop good information security habits.

5. Cyber awareness initiatives coordinated by NMMU

The Information Security Management research group at NMMU has been involved in research in the area of cyber security for more than a decade. During this period, many quality research outputs stemmed from this group, as well as three PhD and about ten masters level students. 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.

5.1 Scope and methodology

The primary methodology followed is that master's and doctoral students conduct specific research projects within an overarching master project. Various products and systems also result from these

projects. Education by means of gaming is a major focus of the group and therefore various forms and types of cyber security games are developed and experimented with.

Another initiative that is currently being addressed is the formulation of a cyber security portal, hosting various different forms and types of related information to provide easy access to all types of related audiences. A formal short learning program (SLP) has been registered at the university to provide basic education to general company end-users. This program has been developed at the university and is currently being ported to a Moodle e-leaning environment. Other outputs that are used in cyber security awareness projects include formal university degrees, research papers, technical projects, games, and content specific websites.

The target audience of the main cyber security project includes all possible groups requiring cyber security education. Taking this into account, the main focus currently being addressed include end-users working in various types of enterprises in both public and well as private sectors, school children and their parents, and the aged. The organisational end-users can stem from any geographical area as the objective is to utilise e-learning technology and Internet based portals.

5.2 Findings pertaining to the specific project

The following are some of the noteworthy results from a survey amongst 1592 schoolchildren in the Nelson Mandela Bay area:

- 5.8% of learners spend more than four hours per day on the Internet,
- 37% use the Internet in their bedrooms,
- 63% do not have to ask permission before accessing it and more than 54% are not supervised when using the Internet,
- 90% said that they use social networking sites (Mxit and Facebook being the preferred sites) and more than 67% access these sites on a daily basis,
- 36% reported that they have experienced some form of cyber bullying and almost half of these reported that did not tell anybody about it,
- 50% said they prefer talking to a friend or peer if they are being cyber bullied, 40% would talk to a parent whilst only 2% reported that they would prefer talking to a teacher, and
- 40% of learners had met someone in the real world to whom they have only chatted to online and 30% said that it had not been who they thought it was going to be.

From these results, it is clear that children, their parents and teachers urgently need to be educated about cyber security.

5.3 The way forward

The educational programme to be rolled out to schools will also be recorded as another success story. The survey conducted at the end of 2010 in the Nelson Mandela Bay area amongst

schoolchildren can be seen as guidance research for children in South African urban areas. The solutions resulting from these efforts should be applicable all over South Africa.

In addition, a project to introduce and assist the aged in utilising Internet related services effectively and securely has been running very successfully for the past two years. From a technical point of view, the system developed to identify and authenticate elderly Internet users using facial recognition, and thereby eliminating the use of usernames and passwords must certainly be seen as another success story.

6. Cyber awareness initiatives coordinated by UP

UP embarks on numerous community-based projects that serve many geographical areas in South Africa. It is compulsory for all students registered at the Faculty of Engineering, Built Environment and Information Technology at UP, to complete a community-based project as an official course in any year of their undergraduate studies. An existing project is called PumaScope, and is the main focus of UP's cyber security awareness initiatives.

6.1 Scope and methodology

PumaScope was launched in 2003 and focuses on the transfer of knowledge in the areas of Computer Science, including basic computer literacy and cyber awareness. Before the project can run every year, extensive planning has to take place. Since the course is presented mainly at schools in rural areas, UP has to annually obtain official permission from the provincial governments where the project is run. The Department of Education then needs to identify needy schools and put the course coordinator into contact with the identified schools.

Each participating UP student needs to spend 40 hours in class lectures and 40 hours of field work in an existing or newly proposed community-based project. The 40 lecture hours focus on the idea of a community-based project and community work in general. After completing the lecture component, projects are advertised and candidates invited to submit Curriculum Vitae. An interview process follows to ensure suitable candidates are selected to take part in Project PumaScope.

A crash course is given by the project coordinator to the selected candidates on how to teach both children and adults - this is crucial so that the students know what is expected from them. The students also sign a code of ethics that binds them to good behaviour and not to bring the UP name in disrepute while out in the field. At this stage the students are ready to embark on their approximate two-week journey out in the field, conveying the project to rural and needy communities.

6.2 Target audience and geographical area

Project PumaScope are mainly offered to rural schools in the Mpumalanga Province of South Africa. Mpumalanga is the province in South Africa that constantly scores lower marks by grade-12 learners compared to other provinces [2]. Therefore, the need to convey such a project is the greatest in Mpumalanga. PumaScope, however, has been offered to needy communities around Gauteng province on a smaller scale.

The target audience can be divided into three main groups: senior high-school learners (grades 10 to 12), teachers and community members. The project has been conveyed at facilities belonging to schools, churches and orphan homes, training the community members in surrounding areas.

6.3 Findings and challenges

Up to date, the project has been conveyed to more than 70 schools and more than 2100 learners, teachers and community members have benefited from the project. One of the major challenges is adequate funding. Although past sponsors include Microsoft and Atos Origin, the sponsorships are solely spent towards travelling costs, accommodation and meals.

The project is sustainable in the sense that a long term relationship is built with the school or institution by establishing a computer club. This club facilitates continuous communication with the school. Some schools have even taken the initiative to present the course originally presented by the UP students autonomously to neighbouring schools. Each beneficiary of the course also receives a certificate upon writing and passing a test after the course. This certificate is accredited by the Department of Computer Science at the University of Pretoria.

6.4 The way forward

One of the visions of PumaScope is to eventually expand to more provinces in South Africa and, eventually, into Africa. This depends on the amount of sponsorship funding that can be secured. Although this particular project does not focus solely on cyber awareness, one of the modules in the course is specifically focussing on cyber awareness.

7. The future of cyber awareness in South Africa

Figure 2 shows a summary of the existing cyber security initiatives in South Africa, as discussed in this paper. Seven distinct user groups in four South African provinces are addressed by the initiatives. The methods employed in the initiatives include games and entertainment, informational websites, post graduate research, short learning programmes, informal and formal lecture-based training and competency tests.

"Cyber space changes so quickly, it's never really the same for very long. With the domain that changes so much like that, it's important - it's almost essential - for us to make progress in the domain as a nation in that we have great education and training" [1]. Following on the plight of George Bartko, chief of the United States National Security Agency Cyber Task Forces, South African cyber security initiatives should work together to provide adequate training and awareness opportunities to all groups of citizens. This is a certain way to ensure that the nation can benefit from various smaller scale initiatives.

By combining the methodologies utilised by these initiatives, it might be possible to arrange for a number of cooperation agreements between the parties involved. This will enable the delivering of a comprehensive package of products that can easily be adapted to be used in all the South African provinces, for all the identified user groups.

8. Conclusion

The paper has shown some of the current South African initiatives to measure and enhance cyber security awareness in different communities, as identified by the CSIR, UFH, NMMU and UP as communities in need of cyber security initiatives. Although not exclusive, this paper provides an indication of some of the cyber security components and topics that should form part of individual

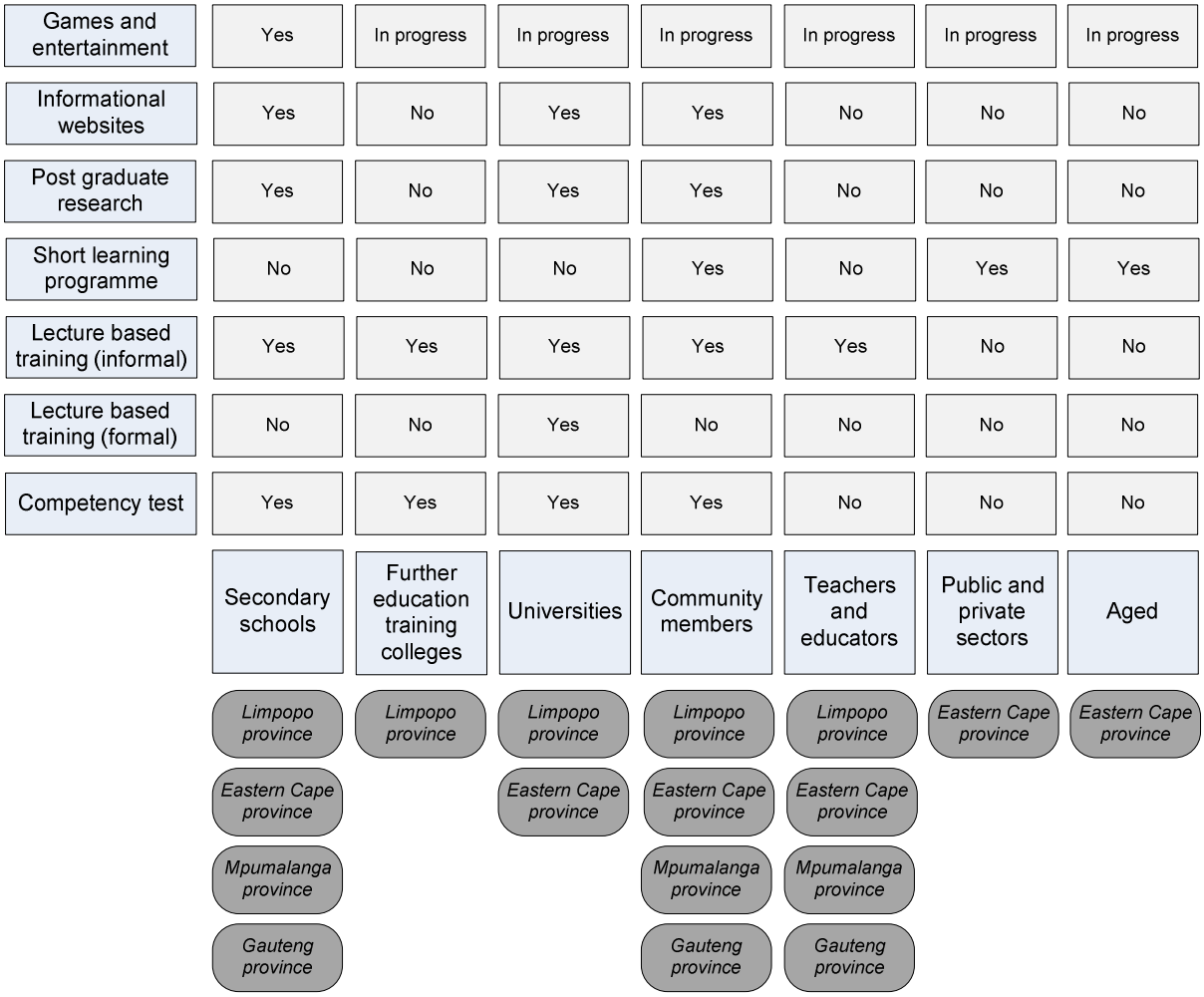

Figure 2: Current cyber security initiatives in South Africa

projects rolled out on a national level. Whilst not directly compared, many of the existing South African initiatives are on par with international cyber security initiatives. Cyber security is a global problem, and thus should be addressed by all nations.

This paper further showed that synergy between different South African entities can contribute to a working cyber security awareness concept that can be easily adapted to be used by countries in Africa in the area of cyber security awareness. Currently, only four of the nine South African provinces are benefiting from these initiatives, but with multi-institutional partnerships, all these initiatives can easily be rolled out to the maximum benefit of both South African and the rest of the African continent.

9. Acknowledgements

Acknowledgement must be given to the CSIR, University of Venda and SAFIPA for their financial support.

References

[1] Bieltz, B. (2011). Panel focuses on future of cyber security. Available from: http://www.dnaindia.com/sport/report_beware-of-phishing-attacks-this-world-cup_1509025 (Accessed 18 February 2011).

[2] City Press. (2010). Matric results for Mpumalanga withheld. Available from: http://www.citypress.co.za/SouthAfrica/News/Matric-results-for-Mpumalanga-withheld-20100105 (Accessed 10 March 2011).

[3] Gilbert, TF. (2007). Human Competence: engineering worthy performance. Pfeiffer, San Francisco, CA.

[4] Mery, Y., Newby, J. & Peng, K. (2011) Assessment; Information literacy; Tests and testing; Reliability management; Learning; United States of America. Reference Services Review, Vol 39 (1) pp 98-122

[5] SAInfo. (2010). Beware of phishing e-mail attacks. Available from: http://www.southafrica.info/ services/consumer/phishing-100210.htm (Accessed 21 January 2011).

[6] SARS. (2011). SARS Phishing Attack. Available from: http://www.sars.gov.za/home.asp? pid=42736 (Accessed 21 January 2011).

[7] Singh, D. (2011). Beware of phishing attacks this World Cup. Available from: http://www.dnaindia.com/sport/report_beware-of-phishing-attacks-this-world-cup_1509025 (Accessed 21 February 2011).