Proceedings of the Eighth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2014)

Towards an Education Campaign for Fostering a Societal, Cyber Security Culture

R. Reid and J. Van Niekerk

Institute of ICT Advancement, Nelson Mandela Métropolitain University
e-mail: S208045820@nmmu.ac.za; johanvanniekerk@nmmu.ac.za

Abstract

The need for information security has moved beyond its traditional organizational boundaries. It is becoming a requirement for all information technology users. Many countries are recognizing this need for their citizens to be cyber aware and secure. Consequently these countries are beginning to implement national cyber security campaigns and efforts. Literature advocates that these campaigns should aim to foster a national (societal) cyber security culture to be truly effective. Currently there are no guidelines for how to foster a cyber security culture at a *societal* level. One of the elements required in a culture fostering process is education. This education needs to be effectively conducted to have a foreseeable, positive result which is measurable. Therefore a scalable, culture fostering campaign is needed. This paper reports a study of an annual cyber security educational campaign which aims to begin fostering a cyber-security culture amongst the youth in the Nelson Mandela Metropolis in South Africa. The objective of studying this campaign is to establish a baseline campaign from which suitable guidelines for a future campaigns (at any scale) may be abstracted.

Keywords

Cyber Security Education, Cyber Security Culture, Youth, Case Study, Awareness

1. Introduction

People, also known as the "human factor", have been established as one of the weakest links in many information or cyber security solutions. These security solutions consist of technologies, processes and people. The technologies and processes within security can be created or drafted to be theoretically secure. However, how truly secure the technologies and processes are depends on whether the people use the technologies securely and/or follow the secure procedures.

People can consciously or unconsciously become a threat to any information security solution (Thomson et al., 2006). When they become a conscious threat it may be with a specific intent or via negligence. Alternatively when they become an unconscious threat it may be for a range of reasons including: a lack of knowledge of security practices; an inability to properly apply their knowledge to their own work role or environmental context; or common negligence. Regrettably as a result of this it is more likely that a breach within an information security solution will occur because of a human fault (the "human factor"), not a technical fault (Mitnick and Simon, 2002).

Within organizations the establishment of an information security culture (hereinafter "ISC") has been widely accepted as a viable counter to this "human factor" threat (Van Niekerk and Von Solms, 2010). The fostering of a culture attempts to address two primary dimensions of the human factor: knowledge, and behaviour (Van Niekerk and Von Solms, 2010).

The establishment of an ISC has traditionally occurred within organizations. This is because in the past the integration of IT into daily activities, and the subsequent need for information security was considered more of an organizational issue. However, the perceived exclusivity of this issue is no longer a valid belief.

The world beyond organizations has become progressively more information-oriented. As a result information security principles have become more applicable to information use in a personal context. Thus at present *all Internet and ICT users* need a basic level of cyber security awareness and knowledge to securely perform their daily activities (Chen et al., 2008; Furnell, 2013).

Security issues relating to the cyber-world now require a coordinated and focused effort from the national and international society, governments and private sectors (Dlamini, 2009). To suit this broader security context a security solution with a greater scope than information security is required. Cyber security is such a solution.

Information security is a process involving the protection of the *confidentiality, integrity, and availability* of *information* from a wide range of threats in order to ensure business continuity, minimize *business* risk and maximize return on investments and *business* opportunities (*ISO/IEC 27002*, 2008). Cyber security also principally involves the protection of information and ICT; however, its scope also extends much further (*ISO/IEC 27032*, 2012).

Cyber security involves the protection of the interests of a person, society or nation, including their information and non-information based assets, which need to be protected from risks relating to their interaction with cyberspace (*ISO/IEC 27032*, 2012; Von Solms and Van Niekerk, 2013). Within this definition humans and their societies are part of the assets needing protection.

Many security specialists and nations are acknowledging the need for populaces to be aware of and educated about being more cyber secure. To achieve this within the current population, and ensure that it continues within the future populaces a "self-renewing" belief which affects behaviour is needed. In an organizational context this need is met through the fostering of an ISC. Similarly in a societal context a parallel cyber security culture ought to be fostered.

This paper represents an initial cycle in a larger action research approach. The paper begins to examine how a cyber security culture could be fostered via education. The findings of this study will begin to demonstrate how to structure a cyber security education campaign which targets needs of a subset of society. The next section will

provide further context and rationalisation for this study. This will be followed by the presentation of the study results, findings and conclusions.

2. Background

Culture is broadly considered to be the overall, taken-for-granted assumptions that a group has learned throughout history (Schein, 2009). ISC builds upon this premise. Many current authors deal with the topic of ISC (Schlienger and Tuefel, Da Veiga and Eloff, Van Niekerk and Von Solms). Most of these authors define ISC in terms of its underlying constituent components. This paper will use the definition offered by Van Niekerk and Von Solms (2010). ISC as an omnipresent concept understood by the people involved in the information security solution(Van Niekerk and Von Solms, 2010). They argue that over simplifying the ISC could be dangerous as an ISC consists of four information security related components:

1. Artefacts: The actual happenings within the organization's daily tasks. This dimension includes the visible structures and processes which were deemed to be "measurable but hard to decipher";
2. Espoused Values: The guidelines (strategies, goals) for what to include in a policy, and consequent ISC to adequately address the business's needs;
3. Shared Tacit Assumptions: The beliefs and values of an individual and collective employees. This includes their unconscious beliefs, perceptions, thoughts and feelings;
4. Knowledge: The necessary and required levels of information security specific knowledge needed to perform the daily business tasks in a secure manner (Van Niekerk and Von Solms, 2010).

The accumulation of how these components develop and interact is considered to be an ISC's effect (Van Niekerk and Von Solms, 2010). Each of these levels can either positively or negatively influence the overall ISC. It may be theorized that a *cyber* security culture would have similar components and behaviors, although the exact details would differ to some extent due to the practices differences in implementation details and context. The method by which the culture is fostered would be important.

A culture can be fostered through either coercion or education. Woodall (1996) argues that, if used, an equitable balance should exist between the degree of coercion used and the reward given, however, generally coercion should be avoided. Within an organizational context, users can be coerced into following security policies and procedures. This can lead to a forced organizational ISC. In a national context it is also possible to use coercion. However, due to ethical and implementation considerations it is a more difficult undertaking and thus less desirable as an approach. Within a national context the educational approach for fostering a culture is preferred. Educational campaigns to teach all of society's users about cyber security issues and practices are thus required.

Many countries have recognized this need to become cyber secure. Part of the process of cyber-securing a country would be the education of the countries citizens about cyber issues and security practices. Many countries have acknowledged this

need for citizen education in their national cyber security policies (Klimburg, 2012 ,pp. 47). However, detail about how this education is to be provided to each society is not provided. This has led to a search for existing guidelines for such an endeavour.

A comprehensive literature review revealed that there are currently no widely accepted, documented guidelines for how to educate users at a societal level about cyber security. There are few generic guidelines for implementing cyber-security and societal educational campaigns even as separate subjects. This leads to two questions: "How can an effective cyber security educational campaign be developed?" and "How can this campaign be made suitable for educating an entire society?"

The first question's solution can begin to be found through adopting some of the fundamental practices from the implementation of past (similarly purposed) informations security campaigns. However, most information security education campaigns occur within organizations therefore the scope and its implementation would have definite difference. For example, in an organisational context education may often be formally (possibly mandatorily) conducted by security experts or human resources. Comparatively in a societal context such a practice would not be well-received. Therefore to answer the second question other methods are necessary. Some methods may be abstracted from the practices of other educational campaigns (of any subject-domain) which aim to educate or raise awareness in general society. Using these premises a number of "trial by error" attempts may be necessary to determine a suitable approach for a societal, cyber-security educational campaign.

The next sections will present a case study of a specific set of such attempts. The next section presents the methodology followed during this study.

3. Methodology

The paper presents a case study (as defined by Creswell (2007)) which spans several years. During these action-research-like cycles of continuous improvement of the process based on lessons learned in previous research cycles is followed. The study follows the case of the annual South African Cyber Security Academic Alliance (SACSAA) educational campaign since 2011. The ultimate aim of the campaign is to foster a cyber security culture via education. This campaign's target audience is the South African youth. However, the presented results were only successfully gathered and analysed from the youth in the Nelson Mandela Metropolis area.

The campaign itself consists of two parts: an education campaign and a poster contest. The campaign aims to first raise the youth's awareness of a number of important cyber safety and security topics specific to the practice of cyber security (humans form part of the assets to be protected). These topics cover the issues commonly acknowledged as being relevant to their own cyber activities and existence. The topics covered the following cyber security issues: stranger danger; browsing, downloading and online activities; cyber citizenship; cybercrime; social

networking; cyberbullying; password and hardware security; viruses and malware; cyber –bullying, -harassment and –stalking; cybersex and finally cyber identity management. The contest is secondly used as an instrument to measure the campaign's impact on the involved youth's awareness levels. Learners are invited to voluntarily create and submit posters (hand-crafted or digitally-created) which promotes awareness of campaign's covered security issues.

To aim of this study is to create an educational campaign component which *effectively* and *measurably* educates the target audience about cyber issues. The researchers selected three measurements to determine the effective impact of the campaign: learner participation; learner internalization of the lessons; campaign memorability through brand association. The first measurement is self-explanatory. It was measured through the empirical data available in the number of entries. The second measurement of internalization, refers to learning which impacts on knowledge, attitudes and behaviour (KAB). An analysis of the posters and the messages/scenarios they depict indicates how educational lessons was perceived and the degree to which they had been internalized (Van Niekerk et al., 2013). The brand association sought to determine whether the campaign itself as an entity was associated with its message. Inclusion of branding into the posters was an indicator.

This section described how the research has been conducted. The next section will present the overviews, results and analysis of each campaign conducted since 2011.

4. Campaigns and Competitions: Results and Analysis

Each campaign formed an iteration of the research cycle which aimed to improve upon the results of its predecessor. This is attempted through the modification of the existent education campaign based on lessons learned in the previous cycles. This section will discuss the implementation and lessons learned in each year's campaign.

4.1. Campaign 1 (2011)

The first campaign was run as a voluntary, distance education campaign. It was a "trial run". The campaign was advertised using professional, promotional flyers. These flyers were distributed via 'snail mail' to schools in the Nelson Mandela Metropolis; and posted on the Nelson Mandela Metropolitan University's campus noticeboards. The pamphlets named topics of interest and encouraged learners to self-study and then participate. Generous cash prizes were offered for the winners.

In total, 3 poster entries were received from NMMU students. Lessons learned were: firstly learners may need to be personally convinced and motivated to become involved. Secondly, to attract school and user attention so as to educate them, a more involved education approach was required. Finally learners may have been more interested in participating if less self-study had been required. Due to the low number of entries no further analysis of the posters was conducted.

4.2. Campaign 2 (2012)

This campaign refocused on solely educating the youth within primary and secondary schools. The invitations were issued via post. Additionally to further attract participants, the researcher personally visited many schools to advertise the campaign and explain its purpose to teachers and learners. The teachers were asked to encourage learner participation in the campaign and competition. Generous prizes were offered for participation in competition.

Several changes were made to the previous campaign approach. To reduce self-study requirements, children were: firstly given a cyber awareness talk by the researcher, and secondly were provided access to relevant material in the form of pamphlets and online topic summary sheets relating to the chosen cyber security issues. Additional resources and reinforcement materials was provided in the format of pedagogically sound games which taught cyber security principles to children through play (Reid and Van Niekerk, 2013). Finally to make the campaign lessons more memorable for the learners, the learners were encouraged to make a cyber safety pledge to themselves and Cyber Sid (a SACSAA partner's campaign mascot).

This campaign was more successful than its predecessor. A total of 217 poster entries were received. Primary school children accounted for 94 of the entries. The remaining 123 entries were from secondary school children. All of the entries received were from the Nelson Mandela Metropolitan area. This is despite having many requests from schools located all across South Africa for competition flyers, educational material and additional information regarding how to enter. In fact, all entries were received from schools that were personally visited by the researcher. Upon analysis of the posters it was found that 66.18% of all of the participants had (in the researcher's opinion) successfully internalized the taught messages.

This campaign showed that a more proactive education approach combined with pedagogically-sound supporting educational material and fun activities engaged more participants. The prizes also potentially attracted participants. Additionally it was found that mascots and other branding should be carefully chosen. Several of the children related the mascot to the topic. Many learners included Cyber Sid in their posters. Finally it was found that the teachers in their support role were vital in assisting to promote the campaign to the children. In future campaigns teachers should be asked to participate more actively in the research.

4.3. Campaign 3 (2013)

This campaign implemented almost all of the previous campaign's procedure. However, a few superficial changes were made. Firstly the Cyber Sid mascot was replaced by the SACSAA logo on all the provided material. Secondly the lectures and support material presented by the researcher was further customised for each school. Upon the teachers' request particular emphasis was placed on the topic/s which most related to problems learners at that particular school had faced. Cyberbullying was considered a prominent issue by many of the schools. Thirdly

the teachers were provided with access to more support material. They could incorporate these resources into their own classes to reinforce the researcher's guest lectures. Finally, less generous prizes than previous years were offered.

This campaign was the most successful thus far. In total 468 poster entries were received. Of these entries 275 were from primary school children and 193 were from secondary school children. The analysis of the posters showed that 84.22% of the participants had (in the researcher's opinion) well internalized the taught messages.

The results of this campaign showed a definite increase in the number of participants. The aggregate of total learners who internalized the message also increased. Unfortunately the number of learners who identified with the mascot/logo decreased.

The analysis of this campaign's results confirmed most of the previous year's observation. Firstly it showed that personalization of the material to emphasize each school's pertinent issues was particularly impactful. For each school that had made a personalization request, the majority of their learners chose that issue as their poster topic. Secondly it showed that increased teacher involvement led to a rise in the percentage of learners who internalized the message. However, this finding is accompanied by a new issue. The level of customization to education material (done by the researcher) cannot be maintained indefinitely using the current educational delivery model. A campaign model which is more scalable is needed.

This section examined the basic results and findings of each year's campaign. The next section will discuss the aggregate findings in terms of the selected impact measurements described in the methodology.

4.4. Overall Analysis and Discussion (Lessons learned)

The ultimate goal of this research is to determine how to educate society and foster a societal cyber security culture. Thus far this study has shown that the campaign is becoming more effective at achieving this objective for the youth societal sub-group. However, the campaign is not as of yet ideal sustainable, scalable and measurably effective. Furthermore some old and new campaign problems are still being resolved. Some campaign success indicators and problems will now be discussed.

The first indicator of campaign effectiveness is the number of participants each year. Due to the various changes incorporated into the campaign participation has annually increased from 3 entries in 2011 to 463 entries in 2013.

This improvement is encouraging, however, it has resulted in a few new issues being identified. The issue of the limited scalability of the current education campaign model is of particular concern. With the current education model's delivery methods and degree of customization (done by the research) only a portion of the total target audience is being reached. This is unacceptable therefore a more scalable education delivery model is required to improve the campaigns advancement.

The percentage of learners who internalized the campaign's lessons are the second indicator of campaign effectiveness. Overall this percentage has increased each year (see Figure 1). The current approach is therefore gaining the learner's attention and explaining the lessons well enough that the learners are adopting the lessons and considering how the issue affects themselves and others around them.

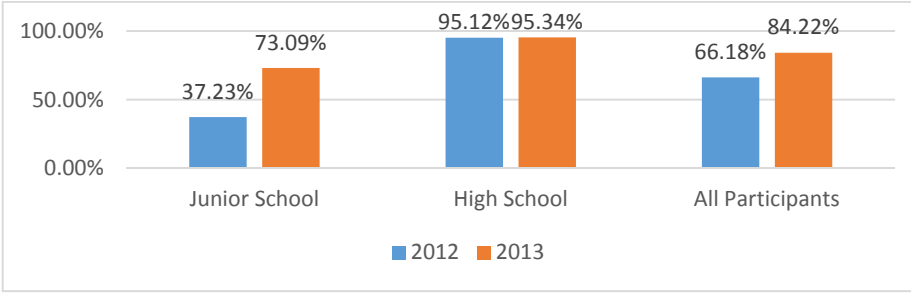

Figure 1: Learner internalization of the taught campaign message

The third indicator of campaign effectiveness is the campaigns memorability through brand association. This is being established through the use of pedagogy and strategic marketing e.g. the use of a mascot. Thus far, each year the brand association has fluctuated based upon the type of branding logo/mascot used (see Figure 2).

This indicator's findings show that the selected branding/mascot must be appropriate for the audience. More of the younger children associated with the character mascot than with logo. The older children displayed the opposite tendency. This indicates that to enable a diverse target audience to associate with the campaign, a more flexible but consolidated branding strategy is necessary.

Overall this study has resulted in four principal lessons being learned. Firstly distribution (logistics) definitely impacts how/if the message is received. The current distribution model is not sustainably scalable. Therefore more suitable model should be sought. Secondly teacher involvement is even more crucial than previously supposed. Teacher involvement caused the levels of internalization and participation to increase. If their involvement becomes more focused, the scalability of the campaign could improve. Security experts are capable of communicating the security material however, the results of their methods are not as successful as those obtained when educationalists are involved. Thirdly suitable, official and age appropriate branding is necessary for campaign memorability and relatability. Fourthly the content of the course is well-chosen, however, the presentation and delivery of the course continuously requires improvement. Involvement from appropriate experts should possibly be sought.

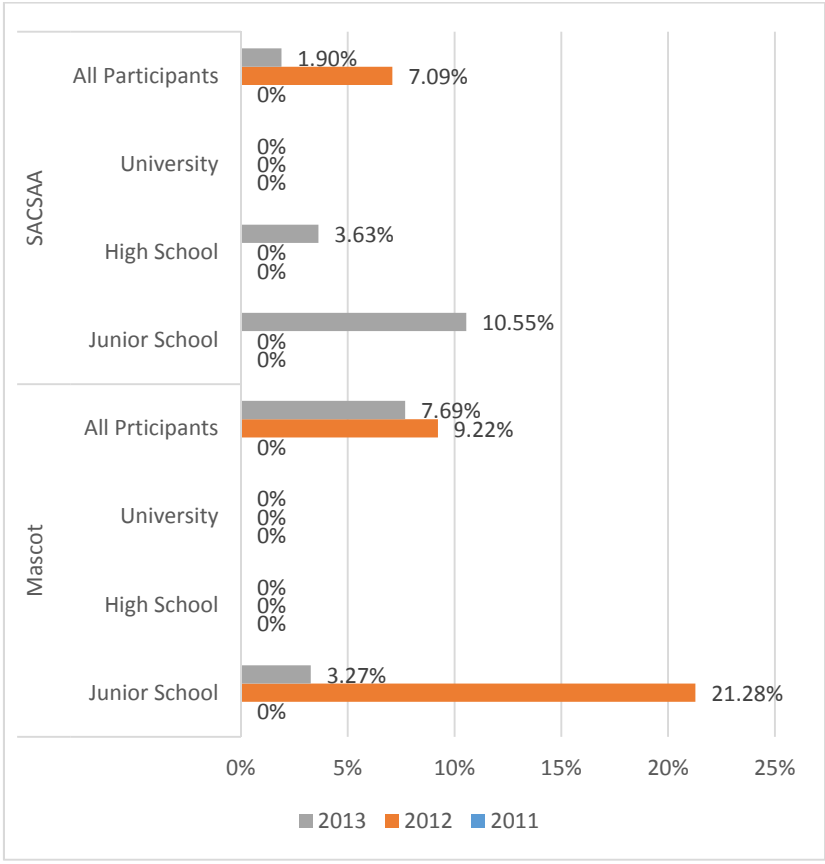

Figure 2: Brand Association for the cyber security education campaign

4.4.1. Upcoming 2014 campaign (future work)

The will be altered to take into consideration the lessons learned in 2013's campaign. An attempt to improve the scalability of the campaign by increasing the educational role of the teachers and decreasing the security expert's presentation role. This year the campaign will follow an adaption of a top-down, organisational culture change approach. Experts will obtain principle top-management support and allow existing hierarchies to further communicate the campaign message. For youth sub-group of society this will be one by getting principal buy in via DOE. Then the security experts will educate the teachers about the campaign topics. The experts will also provide the information about the campaign topics as well as previous campaigns successfully used resources. The researcher will have no contact with the children. The teacher will be expected to customize and present the material to suit their classes and students. Finally lessons learned from this campaign will be used and adapted to guide the development and launch of a parallel campaign which will target another societal subgroup (possibly the organisational sector).

5. Conclusion

The fostering of a societal cyber security culture is vital to educate society about cyber security issues and practices. The lessons learned indicate that to be effective all decisions and implementations of the critical aspects of such a campaign need have a solid theoretical basis. This is particularly important for the selecting and presenting the campaign message.

In this case the most suitable people to ensure that the message is clear is the cyber security subject-domain experts. However, these experts are not necessarily skilled or constantly available enough to any of the other aspects of producing an effective cyber security educational campaign. Therefore the researchers advocate that security expert should determine what to teach users, however, the education and other aspects of the campaign should be done by relevant domain experts. Ultimately the findings or this research strongly suggest that an interdisciplinary approach to education is needed for a cyber-security education needs of a society.

The significance of recognising this need for an interdisciplinary approach could enable the improvement of scalability, quality manageability and continuity possible for a course. Therefore this will aid in developing a culture fostering process which will endure and adapt to change. Further research will focus on developing a framework to enable all involved subject domain specialists to integrate their contributions to create and manage a cyber-security education course which aims to foster a societal cyber security culture.

6. Acknowledgements

The financial assistance of the Vodacom/NMMU and National Research Foundation (NRF) scholarships towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.

7. References

Chen, C.C., Medlin, B.D. and Shaw, R.S. (2008), "A cross-cultural investigation of situational information security awareness programs", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 360–376.

Creswell, J.W. (2007), *Qualitative inquiry and research design*, *Qualitative inquiry and research design*, Sage Publications, Inc, Vol. Second Edi, pp. 73–84.

Dlamini, M. (2009), "Information security: The moving target", *Computers & Security*, Elsevier Ltd, Vol. 28 No. 3-4, pp. 1–10.

Furnell, S.M. (2013), "Security Education: The Challenge beyond the Classroom", *8th World Conference on Information Security Education*, Auckland, New Zealand, pp. 33–38.

ISO/IEC 27002. (2008), *Change*, Organization International Standards.

ISO/IEC 27032. (2012), *Order A Journal On The Theory Of Ordered Sets And Its Applications*, Organization International Standards.

Klimburg, A. (Ed.). (2012), *National Cyber Security Framework Msnual*, *Strategies*, NATO CCD COE Publicaions.

Mitnick, K.D. and Simon, W.L. (2002), *The Art of Deception: Controlling the human element of security*, Wiley Publishing Inc.

Van Niekerk, J. and Von Solms, R. (2010), "Information security culture: A management perspective", *Computers & Security*, Elsevier Ltd, Vol. 29 No. 4, pp. 476–486.

Van Niekerk, J., Thomson, K.-L. and Reid, R. (2013), "Cyber Safety for School Children: A Case Study in the Nelson Mandela Metropolis", *8th World Conference on Information Security Education*, Auckland, New Zealand.

Reid, R. and Van Niekerk, J. (2013), "Back to basics: Information security education for the youth via gameplay", in Dodge, R.C. and Futcher, L. (Eds.),*8th World Conference on Information Security Education*, Springer, Auckland, New Zealand, pp. 1–10.

Schein, E.H. (2009), *The corporate culture survival guide*, Jossey-Bass Publishers, San Francisco, California.

Von Solms, R. and Van Niekerk, J. (2013), "From information security to cyber security", *Computers & Security*, Elsevier Ltd, Vol. 38, pp. 97–102.

Thomson, K., Von Solms, R. and Louw, L. (2006), "Cultivating an organizational information security culture", *Computer Fraud & Security*, No. 10, pp. 7–11.

Woodall, J. (1996), "Managing culture change: can it ever be ethical?", *Personnel Review*, Vol. 25 No. 6, pp. 26–40.