To be published in the IFIP WG 11.8 - 10th World Conference on Information Security Education (WISE-2017)

A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK

Elmarie Kritzinger[1], Maria Bada[2], and Jason R.C. Nurse[3]

[1]School of Computing, University of South Africa
[2]Global Cyber Security Capacity Centre, University of Oxford
[3]Department of Computer Science, University of Oxford
kritze@unisa.ac.za[1], maria.bada@cs.ox.ac.uk[2], jason.nurse@cs.ox.ac.uk[3]

Abstract. This research reports on a study into the cybersecurity awareness initiatives for school learners in South Africa and the UK, which are supported by government, industry and academia. Furthermore, this article provides an overview of similarities and differences between initiatives across countries, and posits as to the reasons why they may exist. The research concludes by presenting recommendations for both countries to improve school cybersecurity initiatives.

Key words: Cybersecurity. awareness. children. nation states

1 Introduction

The impact of cyberspace on society is indisputable. These technologies have permeated every area of our lives and are used to support a vast range of activities, from communication to gaming, business and trade. As these technologies have increased in usage, however, so too has their attractiveness to online predators (e.g. criminals, hackers and child groomers) and their use for unethical and illicit activities (e.g. cyber stalking, illegal trade) [1]. This is a significant security and privacy challenge for society in general, but is especially poignant given the number of children using the Web, and the hours that they spend online.

In a recent study for instance, it was found that 7 to 16-year-olds spend about three hours online daily, but this figure rises to almost five hours when the age range 15 to 16-year-olds are considered in isolation [2]. Moreover, the study found that 67% of youngsters owned a tablet device with access to the Internet. Ownership is a key factor here because it raises the question of whether parents check or even have access (e.g. a security code) to the device. Given the high likelihood that young children are unaware of the various threats online, they are immediately at an increased risk and highly susceptible to attack. This fact has been emphasised by several studies in practice and across academia [3].

This paper focuses on the topic of children's safety and security online, by reflecting critically on some of the existing cybersecurity awareness initiatives for school learners. The research focuses on the awareness efforts present (or absent)

in schools and the reasons for these. Firstly, given that school is compulsory in a majority of countries, it would be one of the best places for awareness training to be provided. There is also the reality that children will be online at school or at home (e.g. browsing or on social media), and as such will be at risk; this is especially true with the vast range of security and privacy risks on the horizon [4].

To set the context for our research, we investigate the cybersecurity awareness initiatives for school learners in South Africa and the United Kingdom (UK). These countries were selected because they would allow us to explore and compare the current state of initiatives in a developed, and a developing, nation. Whilst one would expect developing countries to be more advanced, there is still the question of how much more exactly; also, how do culture, society and industry play a part in these initiatives? Some school awareness research was conducted in respect of these countries separately especially in South Africa [5, 6], but efforts were neither aimed at investigating the complete set of initiatives, nor did they attempt to present actionable recommendations for the range of key stakeholders. This current article seeks to add the most value to existing research by focusing on the current state of initiatives in both countries and reflect on how factors such as culture might define that state.

The remainder of this paper is structured as follows. Section 2 reflects on the relevant research and practice in cybersecurity safety for school learners. This section highlights the range of cyber risks affecting school learners, before continuing to identify the main types of awareness initiatives that may be present in schools. Section 3 considers the current situation as it relates to cybersecurity awareness initiatives for school learners in South Africa and the UK respectively. Section 4 first discusses the key similarities and differences across the two countries before then presenting recommendations for parents, schools and government on how to improve awareness initiatives. Finally we conclude the article in Section 5.

2 Background

2.1 Cybersecurity/safety for school learners

In today's world, school learners grow up within an Information and Communication Technology (ICT) environment and become technology users from their early years. ICTs are integrated in all aspects of their daily lives and are used for the purpose of education, socialising, gaming and information gathering. Recent studies have shown that a growing number of school learners have access to technologies, including devices such as mobile (cell) phones, tablets and desktops [3, 7].

The number of ICT users is growing each year due to the decrease in the cost of devices, increase in access to networks and higher network bandwidth. Another factor to consider is the significant growth of users that have access to mobile devices. Currently, there are more mobile phones in the world than people and 40% of the world's population have access to the Internet [8]. One

group of ICT users who are becoming cyber citizens in their own right are school learners (i.e. school children between the age of 8 and 18) [9].

On the one hand, access to cyberspace provides school learners with a wide range of advantages and benefits which include socialising, access to information and improving their education. On the other hand, however, cyberspace is an unregulated and dangerous platform and school learners could easily fall victim to a range of cyber risks and attacks [10]. Next, we expand on the dangers that school learners may face and discuss a number of the cybersecurity risks present in the online space.

2.2 Cyber risks affecting school learners/youth

There are a number of cyber risks and threats connected to cyberspace that may have a short- and long-term impact on the social, physical and emotional well-being of school learners [11]. According to Stone [7], cyber risks for school learners can be divided into three main categories as depicted in Table 1.

Table 1. Main cyber risk categories (according to Stone [7])

Individuals' intention to harm the learner:	**Learners' exposure to harmful online interactions:**	**Learner places her-/himself in a harmful situation:**
Cyber bullying: trolling, flaming, excluding, masquerading, mobbing, denigrating, outing, harassing, cyber grooming, impersonation, blackmail, cyber snooping, identity theft, social engineering, online predators	Inappropriate content/material, digital reputation ruin, social platforms and chat rooms, viruses, malware, cookies	Illegal file sharing, plagiarism, inappropriate posting online, free downloads, copyright infringements, non-ethical postings of others' material, sexting

Some research has argued that a more youth-centred approach to cybersecurity is long overdue [9]. It is vital that school learners understand their responsibility in protecting themselves and their information in cyberspace. Other cyber-related issues to be dealt with include: protecting passwords; managing privacy settings; adhering to cyber etiquette; meeting in real life people you initially met online; age-appropriateness and digital footprint. School learners should be encouraged and equipped to take responsibility for their own cybersecurity through effective awareness programmes and education.

Considering this wide range of issues, a consolidated awareness approach is needed to enable school learners to gain the knowledge and skills in order to safely interact while in cyberspace. In the next section, our article progresses from theory to practice, and examines the cybersecurity awareness initiatives that have been developed in two countries to educate and protect school learners.

3 Current situation in South Africa and the UK

To scope our current study, we have decided focus on the cybersecurity awareness initiatives in the developing nation of South Africa and the developed state

of the UK. Our work seeks to provide an overview of the various types of initiatives and identify the different sectors (government, industry, academia or education/schools) that drive these initiatives. This therefore supplies the foundation for the detailed comparison and the recommendations provided in Section 4. The methodology that we adopt for our study involves a thorough search and review of existing initiatives in South Africa and the UK, including those present on the web as well as digital and print media. Following this, we critically reflect on these initiatives, their aims, and the sectors which drive them.

To briefly summarise our study's findings, we discovered that South Africa has an understanding of the relevance and importance of cybersecurity awareness for school learners. There are some clear indications of attempts to raise cybersecurity awareness and to establish an effective cybersecurity culture in South Africa. With respect to the UK, several initiatives and programmes are currently being organised to raise cybersecurity awareness, covering various target groups of society, including school learners. These are generally coordinated by the UK's National Cybersecurity Strategy [12]. When it comes to initiatives focusing specifically on school children, it was noticed that some efforts are in place. Furthermore, the public and private sector, academia as well as the schools, are working to establish a cybersecurity culture for school learners.

Table 2. Cybersecurity initiatives in South Africa and UK

Initiatives	**South Africa**	**UK**
School curriculum	Academia	Government, Industry
School workbooks	Academia	Government, Industry, Academia
Teacher training	–	Government, Industry
School ICT policies and procedure	Government, Schools	Schools
Incident handling process in schools	–	–
Awareness material (posters, brochures)	Academia, Industry	Government, Industry
Parent involvement projects	Schools	Government, Industry
One-off initiatives (open days, talks, workshops)	Academia, Schools, Industry	Government, Academia
Web presence	Industry, Academia, Government	Government, Industry
Traditional media presence	Government, Industry, Academia	Government, Industry
Legislation, policy or regulation on cybersecurity in schools	Government	Government

In Table 2 we present our findings including the initiatives currently being undertaken and their main proponents in both countries.

4 Reflections and recommendations

In this section, we reflect on, and present, the key similarities and differences in cybersecurity initiatives in South Africa and the UK. Our approach to this task involved reviewing the data gathered on initiatives and critically comparing the findings from both countries. Based on this reflection, we then sought to identify recommendations for each country on how awareness efforts may be improved.

4.1 Key similarities and differences

In reflecting on the initiatives in both countries, several similarities and differences were identified. With respect to the similarities, it was commendable to find that both countries are making noteworthy efforts to increase cybersecurity awareness in schools and institutions nationwide. This demonstrates an understanding of the range of threats and cyber risks that school learners, in particular, and society in general, are facing. The cybersecurity awareness initiatives that were identified cover areas such as learner training and educational materials (e.g. workbooks and posters by SACSAA, Childnet, the Digital Wildfires project), as well as a range of activities (e.g. one-off workshops and talks by academia and industry) intended to highlight the risks of cyberspace [13, 14, 15]. A few of these initiatives (e.g. Digital Wildfires) have been targeted at specific age-groups to ensure maximum impact once released.

Our research also found that industry played a crucial part in raising awareness among school learners in both countries. In South Africa, the Internet Safety Campaign (ISC) [16] has developed several online resources, and in the UK a plethora of initiatives have been launched, with the UK Safer Internet Centre, the Mobile Industry Crime Action Forum, and the TechFuture Partnership all being involved. Industry involvement is ideal as they contribute expertise and information on a range of current and future technologies.

School-driven programmes were also encountered in our study. This was significant as it demonstrated schools' keenness on promoting cybersecurity and e-safety, even if it was not an obligatory part of their charters. One slight difference here was that whilst e-safety school policies appear to be popular in the UK, uptake in South Africa seemed limited to schools with greater access to funding. This is somewhat understandable given the context of the two nations (a developed versus a developing state). It is encouraging, however, to witness that whenever funding is available, cybersecurity and e-safety awareness appear to be topics that are considered.

Although there are a number of similarities between South Africa and the UK, there are also several differences. To start, the UK government has made a significantly larger effort to incorporate cybersecurity awareness in all parts of society. Initiatives range from national awareness programmes such as Cyber Aware (formerly Cyber Streetwise) and GetSafeOnline to ensuring that cybersecurity awareness is included in the school curriculum. Overall, the contribution by government is possibly the largest difference between the status of cybersecurity in the two countries. By targeting the curriculum and providing a variety

of resources to support school learners and teachers (including specific training), the UK is ensuring that its approach stands the best chance of success.

Some of the awareness efforts from the UK mentioned above can be witnessed in South Africa (e.g. ISC, within industry), but they are not as concentrated, organised or detailed. Also, important areas such as teacher training have not received much attention thus far. While both countries boast a number of initiatives led by industry, the drive by industry-based consortiums in the UK is so substantial that they rival the initiatives of the government in South Africa. This is less than ideal from a government perspective, because contributions by industry often do not last in the long term. There are also questions about the true effectiveness of such programmes if they have not been properly planned or coordinated.

One notable area where South Africa leads the way is in its emphasis on academic research in cybersecurity awareness in schools and in the provision of learning and educational materials. Academics from SACSAA have contributed significantly to the body of research knowledge, and have engaged in the curriculum design for cybersecurity education, workbooks, posters, workshops and school visits. Conversely, academia in the UK does not appear to be involved as much (barring work by the Digital Wildfires group), nor in the efforts towards supporting national awareness campaigns. There is undoubtedly insight from research that could be beneficial in designing and executing such campaigns.

Moreover, the SACSAA workbooks in South Africa are available in multiple languages and through the alliance there are multiple opportunities for outreach in schools and communities. UK academics are involved with outreach (e.g. CAS [17]), but only a few efforts are undertaken towards the creation of workbooks and educational materials. This lack of focus may, however, be the result of the variety of programmes offered by government and industry.

One last point to note about the initiatives adopted by both countries is the influence that culture has had on their design. To consider the UK's GetSafeOnline campaign and the Parents' Corner Campaign in South Africa as examples, it clearly indicates the emphasis on an individualistic approach in the UK (i.e. getting people to think of online security as their own responsibility), whereas in South Africa the emphasis is more on a collective approach (i.e. it is everyone's responsibility to protect one another and society). This is a factor highlighted before (e.g. see [18]), and it can still be noticed in the way that campaigns are designed and conducted. This demonstrates the importance of culture as an overriding factor that should not be ignored.

4.2 Recommendations

From our reflection on the practices of each country, it became clear that both countries have engaged in efforts towards building and enhancing their cybersecurity initiatives within the school environment. There are some areas, however, where improvements can be made and countries can learn from good practice. Below, we present some brief recommendations based on areas where we felt the most value could be added.

Recommendations for South Africa: To consider the case of South Africa first, there is a noteworthy start to the process of ensuring cybersecurity among school learners. Some recommendations for a national plan to improve cybersecurity within the school environment are:

1. Create a national school plan that describes how cybersecurity will be addressed to improve the awareness efforts of all school learners and teachers.
2. Ensure that all schools will implement an ICT policy that includes cybersecurity. This ICT policy must be provided to schools by the relevant government department and must be standardised for all schools.
3. Ensure that all ICT policies in schools are implemented with regular monitoring and evaluation.
4. Provide schools with a clear cybersecurity incident-handling protocol. This protocol should include the details of all the participating organisations that can assist when cyber incidents occur.
5. Provide training for all teachers regarding the following: (a) Cybersecurity awareness for school learners; (b) Age appropriateness for school learners regarding selective topics; and (c) Incident-handling methods if the safety or security of a school learner has been compromised.
6. Collaborate with industry and academia in order to supply the necessary resources for providing cybersecurity education and training for teachers.
7. Establish and implement a parent involvement plan that would allow them to assist with cybersecurity awareness efforts and training.
8. Ensure nationwide exposure to cybersecurity (through social media, traditional media, workshops, open days, posters, and brochures).
9. Create and integrate a cybersecurity curriculum into the national school curriculum. This recommendation aims to incorporate cybersecurity within the "Life Skills" section of the curriculum.
10. Develop awareness-raising programmes, courses and online resources for target demographics, such as school learners, parents and teachers.
11. Involve academia, civil society, and the public and private sector in the development of awareness-raising programmes.
12. Circulate comprehensive and tailored workbooks (including educator guides) that can be used in schools.

For all recommendations mentioned above, the responsibility lies primarily with the government, and particularly the Department of Basic Education, which is ultimately responsible for the school system within the country. Secondary, all schools themselves should be responsible for the implementation and monitoring of policies, procedures and measures set by government departments. It is therefore vital that both the government and schools commit to working together to improve cyber safety. Lastly, industry and academia should provide the requisite assistance to these other sectors to facilitate the transfer of knowledge, skills, tools and research. This would ensure that the recommendations are properly and effectively created, implemented and monitored.

The main focus point to improve cyber safety awareness is to ensure that a national cyber safety skills and capacity building project is provided to all

role-players including government employees and teachers. The starting point to improve cyber safety awareness in schools is to "teach the teachers".

Recommendations for the UK: To enhance the existing efforts of the UK, the following steps are recommended:

1. Maintain and expand the existing awareness programmes (and campaigns) to identify and cover specific target groups.
2. Ensure a strong link between awareness efforts and the national cybersecurity strategy.
3. Enact evaluation measurements to study the effectiveness of the awareness programme in schools at a level where they inform future campaigns (taking into account gaps or failures).
4. Continue to promote a high multi-stakeholder engagement in the design of awareness campaigns, including in academia and civil society.
5. Encourage the private sector to also provide awareness education in order to promote the safe use of their offered services.

A key positive in the UK is that education offerings in cybersecurity range from primary to postgraduate. The Programmes of Study for Primary and Secondary education were published by the Department for Education in 2013 [19]. Internet safety is included in the Programmes of Study for all Key Stages to help ensure that young people are using technology safely. The various projects have been developed in collaboration with key industry partners who provide business cases and ideas for each, and supply industry resources and software for students to use. That being said, concerns have been expressed about whether these offerings are aligned with practical cybersecurity and operational challenges [20]. The government promotes partnerships with various sectors in order to enhance the education of teachers, but still not all teachers are trained in cybersecurity issues. To improve the level of capacity, we also recommend the following:

1. Create compulsory cybersecurity modules for students and teachers.
2. Develop effective metrics to ensure that educational investments meet the needs of the cybersecurity environment.
3. Cultivate partnerships for the development of interfaces to research and innovation and for interaction between universities and the local economy.
4. Develop a centralised platform to share guidance with teachers and parents.

The findings of this research indicate that through the take-up of these recommendations, the state of cybersecurity awareness of school learners in particular and of the UK in general, will be greatly enhanced. Both the Government of the UK and industry already collaborate to establish programmes for enhancing skills and capability in cybersecurity, while national education and skills priorities are informed by broad multi-stakeholder consultation. However, in order to enhance the existing capacity cybersecurity awareness needs to be engrained through all stages of education not only for school learners but also for teachers.

Furthermore, investments should be made both by the public and private sector but also by academia into effective metrics that will ensure that educational offerings meet the needs of the cybersecurity environment. An important step towards this goal would be forming working groups comprised by stakeholders from the public and private sector, academics as well as law enforcement representatives, exploring metrics of effectiveness. Currently, the effectiveness of such existing measurements is often limited due to difficulties in reporting cybercrime. Finally, as mentioned above, the development of a central platform for sharing information and requirements for cybersecurity training provided to teachers and parents can lead to better coordination of the existing efforts.

5 Conclusion

While cyberspace has provided society with a range of opportunities, several risks are associated with it. This is especially the case for younger individuals who may be unaware or too naive to recognise the seriousness of the threat. In this paper, we focused on the topic of school learners' safety and security online, and reflected critically on the existing cybersecurity awareness initiatives. The scope of our work was limited to South Africa and the UK, as we aimed to understand the state of initiatives in a developing and a developed country. This allowed us to assess the levels of maturity in these countries in terms of their awareness programmes, but also to consider the impact of culture and society.

Through our in-depth analysis of South Africa and the UK, we found numerous awareness efforts in play. Both countries boast initiatives launched by the main national sectors (government, industry, academia and schools), with the main difference in the maturity of these initiatives. Given the status of the countries, in some instances this was understandable as the UK government has taken greater effort with awareness in schools. However, in other cases, our findings were unexpected (e.g. in South Africa, academia was considerably more involved in supporting awareness efforts).

Having reflected on the initiatives in each country, this paper set about providing recommendations on how to enhance cybersecurity awareness efforts among school learners. In South Africa, these recommendations concentrated on building capacity for awareness in each sector, whilst in the UK the goal was more towards ensuring concerted awareness efforts that were ingrained and measurable. The conclusion of the research proposes the crucial steps in going forward to ensure that school learners are prepared for the cyber risks and threats that they face on a daily basis. Implementing the proposed recommendations will also have follow-on benefits for the country's economy, given that these learners are the next generation of workers. Future research should focus on similar analysis in different cultural environments in order to identify best practice when it comes to achieving cybersecurity awareness for school learners. Moreover, quantitative work could be conducted to determine the efficacy of the various aspects of these awareness initiatives.

References

1. Symantec Corp.: Internet Security Threat Report (2016) https://www.symantec.com/security-center/threat-report.
2. BBC: Time spent online 'overtakes TV' among youngsters (2016) http://www.bbc.co.uk/news/education-35399658.
3. Livingstone, S., Smith, P.K.: Annual research review: Harms experienced by child users of online and mobile technologies. Journal of child psychology and psychiatry **55**(6) (2014) 635–654
4. Nurse, J.R.C.: Exploring the risks to identity security and privacy in cyberspace. ACM XRDS: Crossroads Magazine **21**(3) (2015) 42–47
5. Reid, R., Niekerk, J.V.: Snakes and ladders for digital natives: information security education for the youth. Info. Man. & Computer Security **22**(2) (2014) 179–190
6. Kritzinger, E.: Enhancing cyber safety awareness among school children in south africa through gaming. In: Science and Information Conference (SAI), 2015, IEEE (2015) 1243–1248
7. Stone, K.: Keeping children and young people safe online: balancing risk and opportunity. Key Messages (2013) http://withscotland.org/download/keeping-children-and-young-people-safe-online-balancing-risk-and-opportunity.
8. Boren, J.: There are officially more mobile devices than people in the world (2014) http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html.
9. Miles, D.: Youth protection: Digital citizenshipprinciples & new resources. In: Cybersecurity Summit (WCS), 2011 Second Worldwide, IEEE (2011) 1–3
10. Furnell, S.: Jumping security hurdles. Computer Fraud & Security **2010**(6) (2010)
11. Byron, T.: Safer children in a digital world: The report of the byron review: Be safe, be aware, have fun. (2008)
12. HMG: National Cyber Security Strategy 2016 to 2021 (2016) https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.
13. SACSAA: South African Cyber Security Academic Alliance (2011) http://www.cyberaware.org.za.
14. Childnet International: E-safety in the Computing Curriculum (2015) http://www.childnet.com/resources/esafety-and-computing.
15. Digital Wildfires Project: (Mis)information flows, propagation and responsible governance (2016) http://digitalwildfire.org.
16. ISC Africa: Internet Safety Campaign (ISC) (2016) http://iscafrica.net.
17. Computing At School (CAS): Events (2017) https://community.computingatschool.org.uk/events.
18. Bada, M., Sasse, A., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? In: International Conference on Cyber Security for Sustainable Society. (2015) 118–131
19. HMG Department for Education (HMG-DE): National curriculum in England: computing programmes of study (2013) https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study.
20. Global Cyber Security Capacity Centre: Cybersecurity Capacity of the UK (2016) https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-uk.