Reviewing National Cybersecurity Awareness in Africa: An Empirical Study

Maria Bada
Department of Computer Science, Global Cyber Security Capacity Centre, University of Oxford
Oxford, UK / Academy for Computer Science and Software Engineering University of Johannesburg,
Johannesburg, South Africa
e-mail: maria.bada@cs.ox.ac.uk

Basie Von Solms
Academy for Computer Science and Software Engineering University of Johannesburg,
Johannesburg, South Africa
e-mail: basievs@uj.ac.za

Ioannis Agrafiotis
Department of Computer Science, Global Cyber Security Capacity Centre, University of Oxford
Oxford, UK
e-mail: ioannis.agrafiotis@cs.ox.ac.uk

***Abstract*—Over the last years, there has been an unprecedented increase in cybercrime globally. Africa is a region with one of the highest rates of cybercrime and significant financial losses. Yet, awareness of risks in cyberspace amongst citizens of African countries is in its infancy and capacity building initiatives focusing on designing and implementing such campaigns are lacking. As part of the Global Cybersecurity Capacity Centre (GCSCC) programme, we visited six countries and assessed their cybersecurity posture based on the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the GCSCC. In this paper, we analyse qualitative data collected by conducting focus groups with experts in awareness campaigns during our visits. We reflect on best practice approaches for developing campaigns and draw conclusions on what the current state of African countries is regarding awareness in risks from cybercrime, what are the main obstacles in combating cybercrime and how countries should identify and prioritise their actions. We believe that our paper contributes in research concerned with how to mitigate cybercrime.**

Keywords-cybersecurity national strategies; cyber threat awareness; risk.

I. INTRODUCTION

Over the last years, there has been an unprecedented increase in cybercrime globally [1] [2]. Africa is a region with one of the highest rates of cybercrime affecting the strategic, economic and social growth development of the region [3]. Reports suggest that, inter alia, estimated costs have soared up to $550 million for Nigeria, $175 million for Kenya and $85 for Tanzania [3]. One of the factors creating a permissive environment for cybercrime is the lack of awareness in the African public regarding risks when using cyberspace [3]. Additionally, the level of development of digital infrastructure in African countries directly influences their security posture. Reports suggest that cyber criminals rely on the very poor security habits of the general population [4] and urge policy makers to engage in awareness campaigns [3] since there is strong evidence that such initiatives can efficiently lower the success rate of cybercrime [5]. More specifically, there are white papers estimating that an investment in security awareness and training can potentially change user's behavior and reduce cyber-related risks by 45% to 70% [5]. It is evident that Cybersecurity Awareness is a very important step in the fight against cybercrime in Africa. For that reason, it is essential for any African country that intends to implement interventions in this area to have a holistic understanding of the level of Cybersecurity Awareness in that country. Towards this direction, there have been efforts to capture the status of Cybersecurity Awareness (understanding on cyber threats and risk, cyber hygiene, and appropriate response options) in Africa [6], and in general, the findings suggest that the absence of awareness campaigns regarding cybersecurity and Internet safety create a lax environment for information security [6]. In this paper, we analyse qualitative data from six African countries that was collected when applying the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cybersecurity Capacity Centre (GCSCC) at the University of Oxford [7]. We reflect on best practice approaches for developing campaigns and draw conclusions on what the current state of African countries is regarding awareness in risks from cybercrime, what are the main obstacles in combating cybercrime and what actions countries should prioritise in order to increase awareness of risks from cybercrime in their population. In what follows, Section 2 provides a literature and best practice review on developing cybersecurity awareness campaigns and existing efforts in Africa. Section 3 provides a brief overview of the CMM and the CMM methodology when deployed in a country. Section 4 describes the results from the CMM reviews in six African countries and our analysis of the qualitative data obtained from focus groups during these reviews. As this paper concentrates on Cybersecurity Awareness, which is one component of the CMM, only the results of this component will be discussed. No countries will be referenced, but a general overview of the outcome will be described. Section 5 discusses the results of our analysis and Section 6 concludes the paper.

II. CYBERSECURITY AWARENESS RAISING CAMPAIGNS

According to the UK Her Majesty's Government (HMG) Security Policy Framework [8], it is government's role to raise cybersecurity awareness within a country. '*People and behaviours are fundamental to good security. The right security culture, proper expectations and effective training are essential. Everyday actions and the management of people, at all levels in the organisation, contribute to good security*'. Awareness is used to stimulate, motivate, and remind the audience what is expected of them [9]. This is an important aspect of cybersecurity policy or strategy because it enhances the knowledge of users about security, changes

 ISBN: 978-1-61208-683-5

their attitude towards cybersecurity, and their behaviour patterns.

A. Developing Cybersecurity Awareness Raising Campaigns

There is an abundance of best practice approaches describing principles in designing and implementing an awareness-raising campaign. Little emphasis, however, was put on how to strategically decide the areas where awareness campaigns should focus. NIST [10] is one of the pioneers in this field. Their framework provides three alternatives on how organisations should be structured, detailing for each category the processes for an effective and efficient campaign. For all three approaches, namely centralised, partially decentralised and fully decentralized, NIST provides information on how a 'needs assessment' should be conducted; a strategy should be developed; an awareness training program be designed; and an awareness program be implemented.

Focusing on the design and implementation of awareness-raising campaigns, literature suggests that successful awareness campaigns need to be a 'learning continuum' [10], commencing from awareness, evolving to training and resulting in education. According to OAS [11], it is of paramount importance that stakeholders from the public and private sector, Non-profit Government Organisations (NGOs), and technology and finance corporations must be involved. Once stakeholders are identified, the next steps in the OAS model provide instructions on how to define the goals of the campaign, the audience it targets and the strategy via which the campaign will be implemented.

Even by following best practise, several difficulties exist when it comes to creating a successful campaign: a) not understanding what security awareness really is; b) a compliance awareness program does not necessarily equate to creating the desired behaviours; c) usually there is lack of engaging and appropriate materials; d) usually there is no illustration that awareness is a unique discipline; e) there is no assessment of the awareness programmes [12]; f) not arranging multiple training exercises but instead focusing on a specific topic or threat does not offer the overall training needed [13].

Perceived control and personal handling ability, the sense one has that he/she can drive specific behaviour, has also been found to affect the intention of behaviour but also the real behaviour [14]. Culture is another important factor for consideration when designing education and awareness messages [15] as it can have a positive security influence to the persuasion process. Moreover, even when people are willing to change their behaviour, the process of learning a new behaviour needs to be supported [15].

B. Cybersecurity Awarness Rasising Campaigns in Africa

A review in cybersecurity policies in African countries [16] shows that awareness raising is key issue either as a separate factor or as part of the role of the proposed National CSIRT. A cybersecurity policy and strategy may not be in place yet for all countries in Africa. However, there are already a number of organisations that have identified the need for continental coordination and increased cybersecurity awareness including the African Information Society Initiative (UNECA/AISI) [17], The Internet Numbers Registry for Africa (AfriNIC) [18], ITU/GCA [19], Interpol, The Southern African Development Community (SADC) [20] and ISG-Africa [21].

There are existing efforts in Africa such as the ISC Africa [22]. This is a coordinated, industry and community-wide effort to inform and educate Africa's citizens on safe and responsible use of computers and the Internet, so that the inherent risks can be minimised and consumer trust can be increased. Also, Parents' Corner Campaign [23] is intended to co-ordinate the work done by government, industry and civil society. Recently Facebook has also announced partnerships with over 20 non-governmental organisations and official agencies from the DRC, Ghana, Kenya, Nigeria and South Africa in support of Safer Internet Day (SID) marked on 6 February [24]. SID advocates making the internet safer, particularly for the youth, and is organised by the joint Insafe-INHOPE network with the support of the European Commission and funded by the Connecting Europe Facility programme (CEF).

Usually, most of official awareness-campaign sites include advice, which usually comes from security experts and service providers, who monotonically repeat suggestions such as use strong passwords. One of the main reasons why users do not behave optimally is that security systems and policies are often poorly designed [25]. There is a need to move from awareness to tangible behaviours.

III. THE CYBER SECURITY CAPACITY MATURITY MODEL FOR NATIONS (CMM)

The CMM of the Global Cybersecurity Capacity Centre (GCSCC) at the University of Oxford is a comprehensive framework which assesses the cybersecurity capacity maturity of capabilities which are foundational to building resilience of a country over 5 different dimensions: 1) Cybersecurity Policy and Strategy; 2) Cyber Culture and Society; 3) Cybersecurity Education, Training and Skills; 4) Legal and Regulatory Frameworks; 5) Standards, Organisations, and Technologies.

Every Dimension consists of a number of Factors which describe what it means to possess cybersecurity capacity. Each Factor is composed of a number of Aspects that structure the Factor's content. Each Aspect is composed of a series of indicators within five stages of maturity. These indicators describe the steps and actions that must be taken to achieve or maintain a given stage of maturity in the aspect/factor/dimension hierarchy. These 5 maturity stages are: 1) Start up; 2) Formative; 3) Established; 4) Strategic; 5) Dynamic. The progressive nature of the model assumes that lower stages have been achieved before moving to the next.

In this paper, we focus on the factor '*Cybersecurity Awareness Raising'*. The Aspects, within this factor are '*Awareness Raising Programmes*' and '*Executive Awareness Raising*' with various Indicator specifications for every Maturity Stage. The Aspect '*Awareness Raising Programmes*' examines the existence of a national

coordinated programme for cybersecurity awareness raising, covering a wide range of demographics and issues, while the Aspect '*Executive Awareness Raising*' examines efforts raising executives' awareness of cybersecurity issues in the public, private, academic and civil society sectors, as well as how cybersecurity risks might be addressed. The CMM model was developed by conducting systematic reviews on best practice approaches which are publicly available, as well as consulting experts from various disciplines.

So far, the CMM has been deployed at the national level (rather than at the company/enterprise level), and 54 countries have been evaluated through engagement and collaboration with international organisations and the host country.

The CMM employs a focus group methodology since it has been acknowledged to offer a rich set of data compared to other qualitative approaches [26]-[28]. Stakeholders are identified based on their expertise in each one of the components of every Dimension of the CMM. Focus groups sessions are led by the CMM Review Team.

IV. CMM RESULTS FOR AWARENESS RAISING IN AFRICA

In Africa, a team from the GCSCC has reviewed and evaluated 6 countries based on the CMM and following the methodology described in Section 3. These countries were selected for a review at the time because they were in the process of drafting a cybersecurity strategy. Therefore, the review would assist this process. These reviews have been conducted during the period June 2015 to January 2018.

Regarding the Aspect 'Awareness Raising Programs' and 'Executive Awareness Raising', 12 focus groups have been conducted in total. The stakeholders who participated in the focus groups are from the following sectors: Public Sector Entities; Legislators/Policy Makers; Criminal Justice and Law Enforcement; Armed Forces; Academia; Civil Society; Private Sector; CSIRT and IT Leaders from Government and the Private Sector; Critical national infrastructure; Telecommunications Companies; and Finance Sector. Each focus group session had approximately 10-15 stakeholders and lasted on average 2 hours.

In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions, stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised.

A. Analysis of maturity level data

Three countries have been identified to be at a start-up stage of maturity, two countries have been identified at a formative stage and one at a start-up stage with few of the indicators from the formative stage of maturity being present.

The results clearly indicate that the majority of examined countries in Africa are identified at a start-up stage of maturity. This translates into lack of a national programme for cybersecurity awareness raising. The need for awareness of cybersecurity threats and vulnerabilities across all sectors is not recognised, or is only at initial stages of discussion. Furthermore, awareness raising programmes (if existing) may be informed by international initiatives but are not linked to a national strategy.

Finally, it was identified that awareness raising programmes, courses, seminars and online resources might be available for target demographics from public, private, academic, and/or civil sources, but no coordination or scaling efforts have been conducted. In the next Section, we provide further details, based on our qualitative analysis, on these initial findings.

B. Qualitative analysis of results

We have transcribed all the recordings from focus groups and conducted a thematic analysis on the qualitative data for each country. We adopted a blended approach (a mix of deductive and inductive approach) to analyse focus group data and used the indicators of the CMM as our criteria for a deductive analysis. The inductive approach is based on 'open coding' meaning that the categories or themes are freely created by the researcher, while the deductive content analysis requires the prior existence of a theory to underpin the classification process.

Excerpts that did not fit into themes were further analysed to highlight additional issues that stakeholders might have raised during the focus groups or to inform our understanding on what the next steps should be for a country.

Overall, we identified eight themes in our qualitative analysis for every country. Four themes were based on the aspects described in the CMM model and four themes emerged from the inductive approach. The themes from the inductive approach pertained information on what actions African countries should implement next. Since these eight themes were common for all six countries, we merged the excerpts for each theme from every country. We further examined these excerpts to identify common areas which hindered progress in cybersecurity awareness raising as well as key actions which countries should implement next to improve their cybersecurity posture in awareness raising.

More specifically, the four main themes that emerged from the deductive approach are: a) the lack of national level programmes; b) the existence of ad-hoc initiatives; c) the relationship between ICT literacy (the ability to use digital technology and tools) and awareness and d) executive awareness. In a similar vein, the inductive approach identified four themes which revolved around the same concepts described in the deductive analysis; the difference being that excerpts in the inductive themes pertained information about recommendations and next steps.

1) Deductive Theme Analysis: For all countries, it is evident that a national programme for cybersecurity awareness raising is absent. In many cases, stakeholders mentioned that '*lack of awareness is an institutional problem, not a user problem*' and also that '*a proper cyber awareness programme is needed*'. The importance for such a

programme was acknowledged across the various stakeholders in all countries reviewed in Africa. A main hindrance for the implementation of a national programme is the general lack of cybersecurity awareness outside the technical communities, which stakeholders pointed that its origin is the low ICT literacy in the population of these countries.

It was further emphasised that awareness-raising programmes need to be developed alongside other capacity enhancements, such as incident response, training for cybersecurity educators, national and organisational cybersecurity policies, etc.

Regarding the initiatives theme, there are ad-hoc initiatives in cybersecurity awareness raising that are supported by various institutions. These are being offered from various organisations such as Facebook while the financial sector, civil society and academia organise programmes for schools to raise awareness. According to a stakeholder, '*some telecommunication companies and banks are engaged in awareness activities which includes messages via the media, directed to end-users, e.g. password security*'.

These initiatives, however, are not yet coordinated at the national level. Therefore, it was widely recognised that a more centralised awareness-raising programme would greatly expand a fundamental understanding of cybersecurity capacity.

Often, civil society actors initiate efforts into targeted cybersecurity awareness-raising. Different stakeholders agree that a '*common ground*' between government, private sector and civil society could enable the proliferation of awareness raising to the broader society. Moreover, often it was mentioned that the government needs to work alongside existing efforts in academia to ensure that new initiatives capitalise from the academic experience. Such synergy is critical to ensure that awareness-raising efforts are efficient and effective.

As often mentioned by stakeholders '*people trust social media and do not expect that someone will harm them, we are brothers!*'. A stakeholder also noted that '*It is common in African countries that mobile phones are used to access the Internet, use social media, for e-banking services etc. but people who use online services are not aware of risks*'. Often, lack of awareness leads to a sense of '*blind trust online. A stakeholder noted that 'users trust social media and think that their information is secure, although often websites are still insecure*'.

Another interesting theme that emerged from the analysis of data is the low ICT literacy rate in Africa. Stakeholders indicated that awareness of the effective use of ICT is still only gaining initial traction and that security is seen as only relevant once ICT and Internet literacy is sufficient.

Regarding the theme revolving around awareness among executives, both in public and private sectors, cybersecurity awareness is very limited, which is one reason why cybersecurity awareness raising is not yet perceived as a priority. This has been identified as an important gap, as executives are usually the final arbiters on investment into security.

Some major telecommunications companies conduct internal awareness raising trainings across all levels, but there is not a publicly available initiative which targets executives. As mentioned by a stakeholder, '*the reason for that is that there is limited awareness for cybersecurity threats and risks in the private sector overall, unless in major international organisations, in particular in the banking and telecommunications sectors which face strategic implications of cybersecurity*'.

It was commonly stated that there is a sharp disconnect between the terminology and priorities of the engineers working in IT systems and security, and those at the higher level seeking to make sound business decisions based on risk.

2) Inductive Theme Analysis: Stakeholders mentioned during focus group sessions that '*aspects of cybersecurity need to be introduced in the school curricula and improve ICT literacy*'. It was also noted that '*even in universities, people are not aware of the possible risks and procure without following standards*'. Integrating cybersecurity awareness efforts into ICT literacy courses could provide an established vehicle for cybersecurity awareness campaigns.

Culture is another factor that can impact the effectiveness of cybersecurity awareness programmes. As seen above, the collectivist cultural aspect that characterises offline behaviour in Africa, is also pertained in online behaviour [29].

Currently, due to the lack of national level awareness programmes, '*being hacked brings awareness usually*' as a stakeholder noted. Therefore, the development of such a programme with specified target groups focusing on most vulnerable users is identified as necessary [30]. Also, appointing a designated organisation (from any sector) to lead the cybersecurity awareness raising programme and engaging relevant stakeholders from public and private sectors in the development and delivery of the awareness raising programme is crucial. As stakeholders mentioned in one of the reviews in Africa '*The government realises that lack of awareness is crucial and recognises the importance of a multi-stakeholder approach towards this goal*'. Moreover, it was noted that '*People access social media through their smart phones and security is the last thing on their mind and that convenience is usually coming first*'.

Regarding the executive awareness raising aspect, developing a dedicated awareness raising programme for executives within the public and private sectors is essential. A stakeholder noted that '*different levels of authority need different kind of awareness in order to promote collaboration as well*'. Currently, executives and

management are being called upon to address cyber risk alongside other risks that businesses face.

V. DISCUSSION

Reflecting on the results presented in Section 4, the lack of a central authority, which is crucial in all modes of operation as presented by NIST model [31], is evident. The absence of such authority prohibits the execution of holistic 'needs assessments', amplifies the difficulties in prioritising the areas in which campaigns should be implemented and renders the design of ad-hoc campaigns by a limited number of stakeholders the only alternative. It is imperative that African countries allocate an authority to conduct a national needs assessment, identify the areas where campaigns should focus first, develop a strategy for how these campaigns will be designed and implemented, and coordinate the ad-hoc efforts of different stakeholders.

Focusing on the design and implementation of awareness-raising campaigns, literature suggests that successful awareness campaigns need to be a 'learning continuum' [31], commencing from awareness, evolving to training and resulting in education. Our results highlight the need of African countries to involve stakeholders which are established in all the aforementioned sectors. Our analysis suggests that the audience of the campaigns should prioritise smartphone users, employees of SMEs and board members. The goals should be to communicate the risks from cybercrime, illustrate the need for better security controls and practices, and the need to establish a chief information security officer (CISO), respectively.

This means that businesses and government agencies should start to take steps to increase their awareness and understanding of cybersecurity with a view of the potential impact on overall business performance. Lack of boardroom expertise makes it challenging for directors and councilors to effectively oversee management's cybersecurity activities.

Cybersecurity awareness should reach all levels and inform all users of the internet – from vulnerable, school-going children to families, industry, critical national infrastructures, governments and the African continent with its unique needs [31]-[34]. This will enhance resilience against cybercrimes and attacks and inform African policy development.

If a country has already developed a national cybersecurity strategy, or is working towards that goal, then linking the development of the programme to that Strategy will facilitate the coordination of different capacities towards the development of the programme and its effective implementation.

Regarding the implementation of these campaigns, there are several organisations with ad-hoc initiatives that could facilitate the design and implementation of cybersecurity campaigns, such as ISC Africa [22] and Parents corner [23]. To conclude, it is worth mentioning that the timing for the development of these campaigns coincides with efforts in African countries to increase ICT literacy. As our findings underline, it is a unique opportunity for all African countries to combine ICT development with cybersecurity awareness. In contrast to western societies, where cybersecurity campaigns endeavour to change the norms on how users currently behave online (behaviour shaped since the inception of the Internet), campaigns in Africa can reflect on best practice and create new norms which will encompass cybersecurity requirements.

Moreover, enacting evaluation measurements to study effectiveness of the awareness programme will not only lead to the assessment of the programme but also identify possible gaps that need to be addressed [10] [30].

VI. CONCLUSIONS AND FUTURE WORK

Several reports are depicting a bleak picture regarding the unprecedented increase of cybercrime in Africa. Yet, efforts to raise cybersecurity awareness in the general public are in an embryonic stage. In this paper, we conducted twelve focus groups in six different African countries to shed light into the current situation and identify critical actions which can significantly decrease the success rate of cybercriminals.

Our results suggest that all six African countries do not possess a national programme for raising awareness, there are extremely low ICT literacy levels which hinder any design of cybersecurity campaigns and that executive members in organisations myopically underestimate the problem. To better defend against cybercrime, African countries need to establish a central authority which will coordinate the existing ad-hoc efforts in awareness campaigns and identify the target groups of these campaigns with particular focus on SMEs, mobile-phone users and executive board members. We believe that African countries have a unique opportunity to combine ICT literacy campaigns with cybersecurity principals and shape the norms of the society towards best practice.

As part of our future work, we intend to explore the effectiveness of a national coordinated cybersecurity awareness programme and how it relates to the actual security posture of a country. Our future work will be based on data from developed countries where the CMM has already been applied, as well as on data collected by other international organisations such as the ITU - GCI [35], Australian Strategic Policy Institute - ASPI [36], The Potomac Institute for Policy Studies (PIPS) - CRI [37], WEF - Global Competitive Index [38] and others.

ACKNOWLEDGMENTS

The authors would like to thank Ms. Eva Ignatuschtschenko, Ms. Eva Nagyfejeo, Mr. Taylor Roberts and Ms. Carolin Weisser from the GCSCC for conducting field work and data collection. We are also immensely grateful to Prof. Sadie Creese and Prof. Michael Goldsmith for their comments on an earlier version of the manuscript.

 ISBN: 978-1-61208-683-5

REFERENCES

[1] Trend Micro: "Is there a budding west african underground market?" https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/westafrican-underground, 2017. [retrieved: July 2018].

[2] O. Tomi: "Cyber-crime is africa's 'next big threat', experts warn". http://www.bbc.co.uk/news/world-africa-34830724, 2015. [retrieved: July 2018].

[3] Serianu: "Africa cyber security report". http://www.serianu.com/downloads/AfricaCyberSecurity Report2016.pdf, 2016. [retrieved: June 2018].

[4] Symantec: "Cyber crime and cyber security trends in africa". https://www.thehaguesecuritydelta.com/media/com hsd/report/135/document/Cybersecurity-trends-report-Africa-en.pdf, 2016. [retrieved: June 2018].

[5] Wombat Security Technologies (Wombat) and the Aberdeen Group: "African union cybersecurity profile: Seeking a common continental policy". https://jsis.washington.edu/news/africanunion-cybersecurity-profile-seeking-common-continental-policy/, 2016. [retrieved:June 2018].

[6] T. Skye: "The last mile in it security: Changing user behaviors". https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/CMM%20revised%20edition 09022017 1.pdf, 2016. [retrieved: May 2018].

[7] Global Cyber Security Capacity Centre: "Cybersecurity capacity maturity model for nations (cmm): Revised edition". https://www.wombatsecurity.com/press-releases/research-confirmssecurity-awareness-and-training-reduces-cyber-security-risk, 2016. [retrieved: June 2018].

[8] HMG: "Security policy framework". https://www.gov.uk/government/uploads/system/uploads/attachment data/file/316182/Security Policy Framework - web - April 2014.pdf, 2016. [retrieved: June 2018].

[9] T. R. Peltier, "Implementing an information security awareness program", Information Systems Security, vol. 14(2): pp. 37–49, 2005.

[10] National Institute of Standards and Technology: "Framework for improving critical infrastructure cybersecurity". https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurityframework-021214.pdf, 2014. [retrieved: June 2018].

[11] Organization of American States: "Cybersecurity awareness toolkit". https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/2015%20OAS%20%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20%28English%29.pdf, 2015. [retrieved: June2018].

[12] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories", African Journal of Business Management, vol 5(26), pp. 10862, 2011.

[13] I. Winkler and S. Manke, "Reasons for security awareness failure", CSO Security and Risk, 7.

[14] I. Ajzen, "Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior", Journal of applied social psychology, vol 32(4), pp. 665–683, 2002.

[15] M. W. Kreuter and S. M. McClure, "The role of culture in health communication", Annu. Rev. Public Health, vol. 25, pp. 439–455, 2004.

[16] I. Dlamini, B. Taute, and J. Radebe, "Framework for an African policy towards creating cyber security awareness", The Southern African Cyber Security Awareness Workshop (SACSAW) 2011, pp. 15-31.

[17] United Nations: Economic Commission for Africa, "The african information society initiative (aisi) - a decades perspective". https://www.uneca.org/publications/african-informationsociety-initiative-aisi-decade2015. [retrieved: June 2018].

[18] AfriNIC: "The internet numbers registry for africa". https://www.afrinic.net/, 2018. [retrieved: June 2018].

[19] International Telecommunication Union: "Towards a common future". https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, 2018. [retrieved: June 2018].

[20] The Southern African Development Community: Global cybersecurity agenda (gca). http://www.sadc.int/, 2018. [retrieved: June 2018].

[21] Information Security Group of Africa: Profile. http://pressoffice.itweb.co.za/isgafrica/ profile.html, 2018. [retrieved: June 2018].

[22] ISC: "Internet safety campaign". http://iscafrica.net/, 2018. [retrieved: June 2018].

[23] Parents Corner: "Digital curfews — what are they & do your kids need one? " https://parentscorner.org.za, 2017. [retrieved: June 2018].

[24] L. Masibulele: "Africa rallies in support of safer internet day". http://www.itwebafrica.com/ict-and-governance/523-africa/242730-africa-rallies-in-supportof-safer-internet-day, 2018. [retrieved: June 2018].

[25] J.R.C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present". In Cyberspace Safety and Security (CSS), 2011 Third International Workshop pp. 21–26, IEEE..

[26] M. Williams, "Making sense of social research. Sage, 2002.

[27] J. Knodel, "The design and analysis of focus group studies: A practical approach", Successful focus groups: Advancing the state of the art, vol. 1, pp. 35–50, 1993.

[28] R. A. Krueger and M. A. Casey, "Focus groups: A practical guide for applied research". Sage publications, 2014.

[29] H. C. Triandis, Cultures and organizations: Software of the mind", 1993.

[30] M. Bada and A. Sasse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", in proceedings of the International Conference on Cyber Security for Sustainable Society (CSSS, 2015) Coventry, UK, pp. 118-131.

[31] E. Kritzinger, M. Bada, and J.R.C. Nurse, "A study into the cybersecurity awareness initiatives for school learners in south africa and the uk", in IFIP World Conference on Information Security Education, Springer, 2017, pp. 110–120.

[32] H. Twinomurinz, A. Schofield, L. Hagen, S. Ditsoane-Molefe, and N. A. Tshidzumba, "Towards a shared worldview on e-skills: A discourse between government, industry and academia on the ict skills paradox", South African Computer Journal, vol. 29(3), pp. 215–237, 2017.

[33] E. Kritzinger, "Growing a cyber-safety culture amongst school learners in south africa through gaming", South African Computer Journal, 29(2), 2017.

[34] E. Kritzinger, "Short-term initiatives for enhancing cyber-safety within south african schools". South African Computer Journal, vol. 28(1), pp. 1–17, 2016.

[35] International Telecommunication Union: "Global cybersecurity index". https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx, 2018. [retrieved: June 2018].

[36] Australian Strategic Policy Institute: "Cyber maturity in the asia pacific region". https://www.aspi.org.au/, 2017. [retrieved: June 2018].

[37] The Potomac Institute for Policy Studies: "Cyber readiness index 2.0". http://www.potomacinstitute.org/images/CRIndex2.0.pdf, 2015. [retrieved: June 2018].

[38] The Global Competitiveness Report: https://www.weforum.org/reports/the-global-competitiveness-report-2017-2018 [retrieved: June 2018].

 ISBN: 978-1-61208-683-5