Cyber4Dev-Q: Calibrating cyber awareness in the developing country context

Abstract

Citizens of the hyper-connected world face tremendous challenges in managing their personal online risks; that is to preserve their cyber safety, cyber security and cyber privacy. Governments allocate significant resources to raising awareness about these three areas among their citizens to equip them to manage their online risks. To ensure maximum efficacy, these endeavours must be able to gauge existing levels of awareness to ensure that awareness-creation drives target population-level awareness gaps. A number of excellent and rigorously developed questionnaires exist for this purpose. However, these may not be as accurate in revealing awareness gaps and issues in *developing* countries. Developing country citizens face a range of context-specific challenges, distinct from those faced by developed country citizens. These are likely to impact their cyber awareness development and maintenance. A context-sensitive cyber awareness measurement instrument designed for such a context has a better chance of revealing particular awareness aspects requiring attention. To meet this need, we developed and validated a cyber awareness questionnaire, the cyber awareness calibration instrument for developing countries (Cyber4Dev-Q), for use in developing countries to measure the cyber awareness of their citizens in all three core cyber areas in a context-sensitive fashion.

1. Introduction

Citizen cyber safety, security and privacy are a global concern among governments, organisations and individuals (GOV.UK, 2020; Blue Turtle Technologies, 2020; Security Awareness Company, 2017; Oliver Wyman Forum, 2021) and governments across the world have formulated cyber security strategies to address the risks in cyber space at national levels (International Telecommunication Union [ITU], 2021). With cyber attacks increasing in frequency (Ponemon Institute, 2017; IBM Security, 2020), online users are likely to fall victim if they are unaware of the risks or do not know how to go about mitigating them (Kortjan & Von Solms, 2013). This reality has led to a widely acknowledged need to improve global citizen cyber awareness.

Compared with developed country citizens, developing country citizens face particular challenges that impact on their general cyber awareness. Ndou (2004) named a number of these, among which the following being relevant for cyber awareness too: the general information technology infrastructure of a country, human capital development and legislative issues. The Cyber for Development (Cyber4Dev) field emerged relatively recently to accommodate the needs of developing country citizens relevant to the cyber domain. It has its roots in the more mature Information and Communications Technology for Development field (ICT4D). Both fields acknowledge that the needs of citizens in developing countries are different from those of citizens residing in developed countries. Hence, Cyber4Dev researchers strive to acknowledge and accommodate the needs of *underserved, under-resourced* and *under-represented* global citizens (Unwin, 2009).

In designing awareness-raising interventions, it must be acknowledged that those living in developing countries have varied and different cyber-related needs, depending on their countries' idiosyncrasies and levels of development (Grobler et al., 2011). Concerning raising cyber awareness, it would be naïve to focus solely on individuals without giving due consideration to their contexts.

Indeed, Masha Sedova, co-founder of Elevate Security, argued that a one-size-fits-all approach to cyber training is bound to be ineffective (as cited in Lewis, 2020). It is unlikely that existing awareness levels can be measured accurately using measurement instruments that have been designed by, and validated in, developed countries. This confirms the need for cyber awareness drives and measurement instruments to be context sensitive, especially when used in developing countries. So far, such a measurement instrument does not exist.

The purpose of this research was thus to develop a context-sensitive cyber awareness measurement instrument called the cyber awareness calibration instrument for developing countries (Cyber4Dev-Q) that would measure cyber awareness in the developing country context by accommodating the needs of the citizens of such countries.

The related literature is reviewed in section 2 of this paper. The research methodology applied is explained in section 3 and the results of the study are discussed in section 4. Questionnaire validation is addressed in section 5 with results in section 6. Lessons learnt and future work are examined in section 6 and 7. The paper is concluded in section 8.

2. Literature review

Wolf et al. (2011, p. 2) defined security awareness as "the effort to impart knowledge of or about factors in information security to the degree that it influences users' behavior to conform to policy". Any awareness-raising endeavour must be able to calibrate itself (Wang et al., 2018) (Figure 1); that is, it must be able to (1) measure the baseline cyber awareness of a community before delivering training and (2) measure the success of the awareness-creating programme afterwards to refine subsequent awareness and training drives (Wolf et al., 2011). Such calibration would ensure that training remains relevant and effective by targeting revealed awareness-deficiency areas (Gundu et al., 2019).

Figure 1: Cyber Awareness Raising Stages

Hence, it would be useful to have a questionnaire that accommodated the needs of individual developing country citizens specifically as outlined in the sections below, with definitions of the three core cyber concepts presented in section 2.1. The Cyber4Dev research field is discussed in section 2.2, the South African context, as the country where the study was conducted, is discussed in section 2.3, other cyber awareness surveys that have been developed are reviewed in section 2.4 and a concluding summary of the paper presented in section 2.5.

2.1 Cyber concepts

It is important to, firstly, to delineate the three related but distinct cyber facets that the instrument should cover, namely (1) cyber safety, (2) cyber security and (3) cyber privacy.

Grey (2011, p. 77) defined *cyber safety* as “the safe and responsible use of information and communication technologies (Balfour, 2005; Beach, 2007), including protection against unsolicited marketing and advertising (Frechette, 2005). Cyber safety teaches children about the positive and negative aspects of ICT (Livingstone et al., 2019), safeguarding against individuals who operate websites, attempt to contact children online, or to organise unsupervised meetings in person with children. Cyber safety education also involves guidance on cyber ethics to form a responsible attitude to the use of ICT” (references embedded in the definition by Grey).

Craigen et al. (2014, p.16) defined *cyber security* as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign *de jure* from *de facto* property rights”.

Westin (1968, p. 7) defined *privacy* as “the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others”. This right is not substantially different in the online domain, so this definition serves to cover both.

Figure 2: Dimensions of the three related cyber concepts

Figure ***2*** depicts the dimensions of the three concepts and their interdependencies. For example, the use of a virtual private network (VPN) as a security measure can prevent snooping and enhance cyber privacy. The use of privacy-preserving tools (PETs) can keep personal details private and enhance cyber safety. Cyber safety and cyber security measures augment each other to keep online users both safe and secure.

In the rest of this paper, the term “cyber” is used to refer to all cyber safety, security and privacy risks and concerns.

2.2 Cyber4Dev

A lack of cyber awareness, knowledge and skills could expose developing country citizens to many cyber risks. The Cyber Risk Literacy and Education Index (Oliver Wyman Forum, 2021) ranks geographies on five categories in a cyber context, namely public motivation, government policy, educational system, labour market and population inclusivity. The index shows that citizens in some countries have limited cyber risk literacy and that various countries do not prioritise nor assess their cyber risk education needs. The index clearly illustrates that developed countries such as Switzerland, Singapore, the United Kingdom, Australia and the Netherlands are at the top of the index. Several developing countries are ranked lowest, namely Brazil, Mexico and India, with South Africa being the country with the lowest cyber risk literacy out of the 50 assessed countries. There is thus a clear need to prioritise and assess the cyber awareness and needs of developing countries.

The Cyber4Dev field emerged to address the needs of developing country citizens. This field acknowledges that developing countries face a different spectrum of cyber security challenges. Public awareness of cyber security is low, with internet users having neither the necessary awareness nor the skills to protect themselves from online and mobile security risks (Makoni, 2020). Developing countries often do not have the same cyber legal frameworks, policies and laws. Moreover, African countries in particular are characterised by low levels of digital literacy and weak cyber security systems with few operational Computer Emergency Response Teams (CERTs) (Calandro & Berglund, 2019; Van der Spuy, 2018). According to a United Nations Economic Commission for Africa policy brief, issue NTIS/002/2014, Africa faces a number of internet-related obstacles, with most governments on the continent lacking the technical or financial ability to target and monitor most of these. That is exacerbated by a lack of computer skills with only half of African schools including it in the school curricula compared with 85% globally (Kandri, 2019).

A number of cyber-related interventions such as training sessions and workshops have taken place in developing countries. These are often arranged or sponsored by developed countries. For example, the European Union (EU) and the Council of Europe established the Global Action on Cybercrime (GLACY) and its extension, the Global Extension on Cybercrime Extended (GLACY+) ran cyber crime and policy workshops in Southern Africa (Global Action on Cybercrime [GLACY], n.d.), while the ITU operated cyber crime workshops in the Comoros (ITU, 2014) and Malawi (Jamil, 2014), and also engaged in activities in Botswana, Eswatini, Malawi, Tanzania and Zambia (Global Forum on Cyber Expertise, 2019). In addition, the Cyber Resilience for Development Project funded by the EU (Cyber4Dev, n.d.) was launched in Botswana and Mauritius in 2018 to enhance cyber resilience.

However, these endeavours would not have had access to a context-sensitive awareness measurement instrument specifically tailored to the developing country context, which might have complicated calibration.

2.3 South Africa

South Africa, as the developing country where this research was carried out, faces a number of cyber risks exacerbated by low levels of cyber awareness (Bada et al., 2019; Oliver Wyman Forum, 2021). The country has one of the highest probabilities of data breaches, with 36% of internet users already having experienced some form of cyber attack (Ponemon Institute, 2017). Only 40% of data breaches are attributed to malicious attacks, which implies that human error or lack of cyber knowledge could account for a large number of local data breaches.

The South African government aims to connect its citizens by supporting free wireless internet (Wi-Fi) in a number of cities (City of Tshwane, 2020). Moreover, statistics show that the number of smartphone users in this country have been estimated to reach 26.3 million by 2023, giving even more people access to cyber space (Statistics South Africa, 2020). Cyber awareness is, therefore, critical in ensuring that citizens can benefit from the information age while taking measures to address threats and reduce vulnerabilities. To date, no practical plan has been formulated to achieve this (Sutherland, 2017).

South Africa faces a number of specific challenges (Surbhi, 2020; 9 major problems facing South Africa - and how to fix them, 2011; McDowell, 2010), namely (1) low per capita income, (2) poverty and unemployment, (3) inequality, (4) a low standard of living, (5) literacy (low education levels), (6) multiple languages, (7) primarily a younger population, (8) lack of health and safety infrastructure, and (9) limited public service performance.

Many of these potentially impact citizen cyber awareness and relevant skills development, as illustrated by the Cyber Risk Literacy and Education Index that shows South Africa as scoring low across all categories, including that of cyber-risk awareness and educational inclusivity (Oliver Wyman Forum, 2021).

Figure 3: South Africa's Challenges (Map by Allice Hunter from: https://commons.wikimedia.org/wiki/File:South_African_provinces_by_HDI_(2017).svg)

South African academics are actively supporting cyber-awareness-raising efforts (Venter et al., 2019; Nagyfejeo & Von Solms, 2020; Aldawood & Skinner, 2018). Even so, rural and developing communities remain vulnerable as they are often not aware of or ill-equipped to deal with cyber threats due to one or more of the factors depicted in

Figure ***3*** (Grobler et al., 2012). Improving cyber awareness is a particular challenge in South Africa because of the high unemployment levels (Trading Economics, 2021) accompanied by an especially low drive towards cyber literacy and unequal access to technologies and education.

The South African context differs from any developed country context. That being so, one should acknowledge the impact of the developing context in designing a Cyber4Dev-Q to ensure that the instrument measures cyber awareness as effectively as possible. In essence, while cyber safety, security and privacy principles remain the same across the planet, context-sensitive aspects that inform cyber awareness interventions should be built into cyber awareness drives. Weaving the developing country context into the Cyber4Dev-Q would enhance its power to reveal context-specific aspects that should be addressed by future cyber initiatives in addition to the usual cyber concepts.

2.4 Cyber awareness measurement instruments

Tsohou et al. (2008, pp. 225) argued that "analysis reveals that security researchers, practitioners and managers may be frustrated with security-awareness efforts, since there is no clarification of many issues of concern". In this regard, various studies have been conducted to identify "best practice" in measuring security awareness. Table 1 provides an overview of prominent instruments that have been used to measure cyber awareness in the research literature. Column one provides the authors, followed by column two that includes a description of the questionnaire or questionnaire name. The comprehensiveness column indicates whether the questionnaire meets the three requirements of the calibration instrument, namely cyber safety, cyber security and cyber privacy. The individual focus column reflects whether the questionnaire is targeted at the general end user or citizen, as opposed to an employee in a workplace context. The country context-sensitive column indicates if the questionnaire is developed for a specific country context and the last column shows in which country the study was conducted.

All fail on at least one of the requirements. For example, Kruger and Kearney (2006) developed a security awareness program. However, their intervention was not targeted at individual citizens, but rather aimed at a workplace context. Egelman et al. (2016) focused on the development and validation of the security behavior intentions scale (SeBIS). While their questionnaire covered a range of cyber security topics, it did not include cyber-safety concepts. Parsons et al. (2017) developed the human aspects of information security questionnaire (HAIS-Q). Their questionnaire's questions also related to the workplace context and was validated by Australians; that is developed country citizens. The HAIS-Q has been used in various studies, but in an organisational context (Dharmawansa & Madhuwanthi, 2020; Saridewi & Sari, 2020; Lamp, 2017; Hadlington et al., 2020). Cindana and Ruldeviyani (2018) applied HAIS-Q in an organisational context in Indonesia and found that employees required more awareness of internet usage. Similarly, Zulfia et al. (2019) also used HAIS-Q in an organisational study in Indonesia with recommendations focusing on organisational improvement of awareness of information security policies and technology. While these two studies were conducted in a developing country the context related to employees in a workplace setting. The Cyber Risk Literacy and Education Index (Oliver Wyman Forum, 2021) highlighted the fact that in various geographical regions awareness and teaching of cyber risks are driven by organisations with governments lagging in this regard. This resonates with academic research in cyber awareness measurement instruments, which are, to a larger extent, deployed in organisational contexts as opposed to the general citizen or a community. While some studies used or developed a cyber awareness measurement instrument focusing on the general user or individual (Velki & Šolić, 2019, Egelman et al., 2016), the questionnaires used were not inclusive of cyber safety, cyber security and cyber privacy, as illustrated in Table 1.

A number of researchers have published questionnaires for the purpose of measuring the culture of security (Hayden, 2015; Schlienger & Teufel, 2005; AlHogail, 2015; Da Veiga, 2018), but these do not focus on gauging cyber awareness, nor are they tailored to the needs of the individual but rather aimed at an employee in an organisational context. There is thus a need for a cyber awareness questionnaire that is comprehensive, individual focused and developing country specific.

Table 1: Existing Cyber Awareness Measurement Instruments (•=satisfies; Ø=fails)

2.5 Summary of requirements for the questionnaire

In summary, it is essential to ensure that cyber awareness drives achieve their goals when they are carried out. That implies a need to assess awareness both before and after such drives, which would ensure targeted, relevant and topical training accommodating the developing country context, thus confirming the need for a questionnaire meeting the following requirements:

Comprehensive: incorporating constructs to measure awareness of all three cyber concepts (given that the concepts and required precautions differ substantively – section 2.1).

Country context-sensitive: accommodating the development-level context of the country of residence where cyber literacy is low and where cyber risk education of vulnerable groups (such as native language speakers) is not necessarily prioritised (accommodating the context and challenges of the underserved, under-resourced and under-represented – section 2.2).

Individual focused: targeting individuals as opposed to employees or organisations – section 2.3.

3. Research methodology

The research methodology section firstly presents in section 3.1 the development of the measuring instrument being the Cyber4Dev-Q. The research method, being a survey, is discussed in section 3.2 followed by an overview of the sample and data collection in section 3.3.

3.1 Developing the Cyber4Dev-Q

This research study was conducted in South Africa. Hence, South Africa’s context as a developing country had to be considered for the development of the questionnaire. To ground our questionnaire in that context, we consulted the *Cyber Security Awareness Workbook* published by the South African Cyber Security Academic Alliance (SACSAA, n.d) to educate school children about cyber topics (cyber safety, security and privacy) (Kritzinger et al., 2017). This workbook covers a wide range of topics and focuses on content that is relevant to individuals starting to learn about cyber topics, specifically in a developing country context. Various topics from the SACSAA workbook were used to ensure that all three core cyber concepts were covered: (1) cyber safety: protecting yourself, (2) cyber security: protecting your device and securing your information, and (3) cyber privacy: controlling disclosure of your information. The online etiquette topic in the workbook was excluded in the Cyber4Dev-Q, since the focus of this research related specifically to cyber safety, security and privacy risks and controls and not to etiquette. The *Cybercrime Survival Guide* (Wolfpack Information Risk, 2018), which was developed in South Africa, was also consulted. This guide's aim is to raise awareness of the potential cyber risks that South Africans face. It also provides guidelines to inform end users. We furthermore reviewed other awareness-raising questionnaires to ensure that all pertinent cyber-related aspects were covered (Parsons et al., 2014; Egelman et al., 2016) and studied South African government statistics and news reports reporting on cyber-related crimes and issues in South Africa.

Table *4*, Appendix A, consolidates our findings as well as the themes and theory for the items included in our questionnaire. The citations included refer to the source of each question. The questionnaire statements were phrased from an individual, as opposed to an employee, perspective. For example, when recommending reporting, the advice was that it should be directed to a local authority or cyber group in the community that would be able to provide support at an individual level instead of to the information technology department of a relevant organisation.

The Cyber4Dev-Q comprises three sections:

Context questions to understand the context such as what devices respondents use and for what purpose, where they currently obtain information about cyber security and their preferred communication methods.

Cyber awareness questions adapted from the SACSAA themes and categorised according to cyber safety, cyber security and cyber privacy, as well as questions tailored to developing country challenges.

The SACSAA themes were used to develop each of the questions in the Cyber4Dev-Q as depicted in Table *4*, Appendix A.

Demographic questions to profile the respondents such as gender, age, language and qualification levels.

The questions and their application to the different cyber concepts are depicted in Figure **4**.

Figure *4*: Allocation of questions to Cyber Concepts and co-dependencies

An introduction letter, information document and consent form were included with the questionnaire. These explained the objectives of the research, confirmed that responses would be anonymous, that participation was voluntary and that participants could withdraw at any time (Oates, 2005). Ethical clearance was obtained from the researchers’ university for the research study and data collection.

A pilot study was conducted at a community engagement event hosted at the university during which participants from a developing community were trained in general computer skills. In this pilot study, 17 participants completed a hard copy of the questionnaire and provided feedback on how easy the questions were to understand and the length of the questionnaire. Only minor changes were made and background questions were refined based on the feedback.

3.2 Survey method

A positivist paradigm was applied to establish measurable facts about the cyber awareness in a community in line with the view that using a quantitative approach (Saunders et al., 2009) is effective when the intention is to describe the attitudes or opinions of a population (Creswell & Creswell, 2017). Surveys are an accepted research method for use in information systems research (Oates, 2005) in that they are cost-effective and allow for the use of large samples (Brewerton & Millward, 2001). Moreover, they support the testing of the validity and reliability of the measurement instrument, in this case the Cyber4Dev-Q (Saunders et al., 2009). A hard copy survey method was applied this study and the surveys were hand captured. The Statistical Package for the Social Sciences (SPSS) was used to perform descriptive and inferential statistical analysis. For the purposes of this study, construct validity was tested using factor and item analysis, and the reliability of the measurement instrument was tested using Cronbach’s alpha.

3.3 Sample and data collection

Data were collected during a Chance2Advance event presented at the Ebenezer African Methodist Episcopal Church in Atteridgeville. This annual event takes place to communicate with, educate and enrich participants through a variety of workshops. Atteridgeville is home to a population of 64 000 people spread over a 9.84 km^2 area. The population density is 6 500/km, which is more than the 500/km used to classify rural areas. As a result, Atteridgeville is deemed to be an urban area. Due to the legacy of apartheid, Atteridgeville was previously underdeveloped and segregated from other urban areas. Today, its population comprises predominantly black Africans (99.1%) (Statista, 2020). Problems experienced in the community include high poverty levels, a lack of land for expansion and inadequate social services (City of Tshwane, 2014). The 2011 census indicated that just over 50% of the community has access to the internet (Statistics South Africa, 2011).

Residents who attended the community workshop session hosted by the university were asked to complete the hard copy survey. A total of 160 people attended this cyber workshop and 158 completed the Cyber4Dev-Q. This is referred to as purposive sampling in terms of which a targeted sample is used to meet the research objectives (Saunders et al., 2009).

Refer to Table 2 below for a demographic profile of the respondents. Not all respondents answered the demographic questions. Hence, the total number of responses is less than 158 in some instances. Interestingly, 66% were unemployed at the time of the survey, while 14% were students. The 2011 census data indicated that the community had a 22% unemployment rate. While unemployment is now higher across South Africa at 29% (Statistics South Africa, 2019), it is possible that the workshop participants were available during the day because they were not employed. Such high unemployment levels suggest that they do not have access to cyber awareness training and education, which would be delivered by employers.

Table 2: Demographics of Respondents participating in the Chance2Advance Event hosted in Atteridgeville

4. Results

The data gathered in the Atteridgeville community showed the profile of the community as being mostly generation Y, with the majority in possession of only a school qualification and everyone owning either a mobile phone, laptop or tablet. The content and cyber awareness question results are discussed below.

4.1 Content question results

The answers to questions in the content section of the questionnaire indicated that all respondents used a mobile phone – mostly for phone calls (95%), for instant messaging such as SMS or WhatsApp (82%), to browse the internet (77%) and to access social media sites like Facebook or Twitter (73%). A number of them used their mobile phones to send e-mails, play games or watch videos, and 47% used their phones for internet banking. Not all respondents had access to a home computer or tablet, but those who did (home computer 53% and tablet 44%), used these for a variety of online activities. The word “clouds” (see Figure **5**) reflects the activities that respondents indicated under the “other” option for the use of their mobile phones, tablets and home computers, respectively. Listening to music and watching videos are key activities, while some also use it for work related activities. Respondents engaged in a variety of online activities and were therefore exposed to cyber-related risks, in particular the protection of the devices themselves, with 80% of respondents indicating that their mobile phones had been stolen in the past and 14% indicating that their tablets had been stolen. The respondents reported that they had learnt about cyber topics at school (33%), nowhere (32%), in newspapers (29%) or from their friends (25%).

Figure *5*: Word clouds with usage of devices

The majority of respondents expressed a preference for workshops (58%) or face-to-face discussions with experts (48%), followed by the internet (44%) as means to receive future communication on cyber topics. When asked whether they could recommend other preferred methods for cyber communication, respondents mentioned school, e-mail, Facebook, the community and the church.

4.2 Cyber security awareness question results

A summary of the key results of questions 17–53 (refer Table 5, Appendix A) is presented below under the three themes incorporated in the questionnaire.

Cyber safety:

The majority of respondents were aware of the risk of being stalked (79%) or bullied (78%), with 51% having experienced unwanted sexting and 52% having friends who had experienced unwanted sexting or cyber bullying (47%). Only 32% of community members knew how and where to report a cyber-related incident or crime. Sixty-eight per cent said that they had never fallen victim to such crime. That could be because they were unaware that they had been exposed to such attacks.

Cyber security:

Confidentiality: There seemed to be general awareness of the need to protect information as 75% of respondents reported not giving out their personal information to online gaming websites. They also did not respond to unwanted communication or messages from strangers (72%) and did not post information about their friends (68%).

Availability: There seemed to be a good understanding of the risks pertaining to information, with a high percentage of respondents regarding backups as important (93%) and understanding the risk associated with providing personal information in response to an e-mail of unknown origin (81%).

Access control: Most community members (83%) indicated that they used a password on all their devices and made use of upper case, lower case, special characters and numbers (69%). They were also aware of anti-virus software (61%), but only 48% had installed that on their devices. From a physical security perspective, only 57% had access to a safe place to lock away their electronic devices. The latter resonates with the challenges faced by low-income citizens in developing countries.

Precautions: There was awareness among respondents that their devices could be infected with a virus (86%), that criminals could access their devices (79%) and that their devices could be implicated in cyber crime (75%).

Cyber privacy:

Some participants were aware that their personal information (62%) or identity (63%) could be stolen via cyber space. The majority lacked awareness of website privacy policies, as only 43% knew where to find such policies. Only 50% knew how to change their default privacy settings and 59% indicated that they understood privacy policies. The respondents believed they were safe in cyber space and could do anything they wanted to as long as they remained anonymous or used a fake name (58%). From a cyber safety and forensic perspective, this perception is worrying as end users can be traced to an internet protocol (IP) address unless they are using a virtual private network (VPN). Only 48% believed that it was unacceptable to post or share inaccurate or incorrect information online.

5 Questionnaire validity

5.1 Exploratory factor analysis

An exploratory factor analysis (EFA) using the SPSS was conducted on questions 17–53 in the Cyber4Dev-Q. The data were subjected to Bartlett's Test of Sphericity and the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) to test the aptness of the sample for the EFA (Kaiser & Rice, 1974). Bartlett's test should be significant ($p< 0.05$) to indicate sampling adequacy (Bartlett et al., 2001). In this research study, Bartlett's test was significant at $p<0.00$, providing evidence of sampling validity.

According to Kaiser and Rice, 1974, the KMO should be 0.60 or higher to proceed with factor analysis. Six factors with a KMO value of 0.670 were identified (Table 3). The authors recommended retaining all factors with an Eigen value greater than one (Eigen values represent the amount of variation explained by a factor, and a value of one represents a substantial amount of variation). Here, the Eigen values for all six factors were higher than one, thus suggesting that they could be extracted (Kaiser & Rice, 1974).

Only items with a value above 0.4 were deemed meaningful and thus retained (Gerber & Hall, 2017). Q23, Q33, Q35 and Q53 were therefore removed. The Cronbach's alpha values were all above 0.6, which is deemed acceptable (Gerber & Hall, 2017). Table 3 outlines the six new factors as per the EFA, the new names of each factor, the corresponding question numbers and the Cronbach’s alpha for each factor.

Table 3: New Factors and Cronbach’s Alpha Values

5.2 Cyber4Dev-Q improvements

To improve the Cyber4Dev-Q based on the outcome of the EFA in the SPSS, more items can be added to factors 4 and 6 to have at least three items per factor (O’Rourke & Hatcher, 2013). The questionnaire could also be adapted based on changes in technology and threats perceived by the community, such as the inclusion of firewalls, which might not be relevant to a community using mainly mobile phones (see Q19 and Q20). Similarly, e-mails can be spoofed, which means that an individual might not receive e-mails from unknown sources (see Q26), but this might well apply equally to users of mobile phones in the context of cyber bullying or victimisation. The suggested changes to the questionnaire are included as new factors in Table 5, Appendix A, next to the applicable statements. The six new factors are listed below with a short description of the purpose of each based on the questions grouped per factor in accordance with the EFA.

F1: *Cyber safety and privacy risk awareness*: Perception about the risks and threats in cyber space pertaining to safety and privacy.

F2: *Cyber security protection*: Technical controls for protection in cyber space.

F3*: Personal cyber safety*: The behaviour to protect oneself and others in cyber space.

F4: *Cyber safety risks*: Personal experience of cyber risks.

F5: *Cyber privacy actions*: Actions to protect personal information of oneself and others in cyber space.

F6: *Cyber security for passwords*: Focusing on secure password practices in cyber space.

6 Discussion

It clearly cannot be assumed that all rural and urban South African citizens have the necessary cyber-related awareness and skills. Knowing what a firewall or anti-virus software is, or understanding the meaning of security or privacy policies on websites might appear to be common knowledge (Wilby, 2010). However, while that might be a valid assumption when it comes to security experts or employees who have received cyber awareness training delivered by their employers, it is not common knowledge among all computer users, especially not among those living in developing countries.

Our investigation confirmed that developing country citizens require a context-sensitive approach to address the risks they face from cyber space. The results of this study furthermore confirmed the need for targeted cyber awareness and training presentations or workshops to be delivered by experts in South Africa. They also substantiated the special challenges faced by developing country citizens, confirming the need for a questionnaire that acknowledges their specific challenges and is designed to accommodate those. It can be concluded that the Cyber4Dev-Q satisfied such specific challenges as follows:

Comprehensive: The Cyber4Dev-Q incorporated constructs to measure awareness of all three cyber concepts: cyber safety, cyber security and cyber privacy (Figure **4** and Table 5).

Country context-sensitive: Context-specific questions based on the South African context were included and the validation process revealed the importance of these questions in understanding the challenges of cyber awareness (Figure 5).

Individual focused: No organisational-context-specific questions, particularly related to the reporting of incidents, were included.

6.1 Practical implications

Results obtained through the Cyber4Dev-Q highlighted the following areas requiring future cyber-awareness-raising focus:

In a *developing country context*, the focus should be on reporting, language, delivery method, ethics and devices.

Reporting: Citizens must be made aware of where and how to report cyber-related crimes and incidents; that is awareness of the channels that exist in South Africa for that purpose (public infrastructure issues.)

Language: South Africa has eleven official languages with very few citizens using English as their first language. The language used for presentations and materials must be sensitive to this reality. For example, as Sesotho was the first language of most respondents participating in this study, future workshops in their area should also be delivered in that language. Security awareness drives must be sensitive to the demographic profile of the community (multiple languages).

Delivery method: Electronic communication such as monthly awareness-raising e-mails and social media platforms like Facebook can be utilised and distributed via existing community structures (e.g., churches or schools). Workshops, including face-to-face presentations, are preferred and would thus be the optimal delivery mechanism in this developing country context (low literacy levels).

Ethics: The sharing of inaccurate or incorrect information in cyber space requires attention (different laws).

Device: Awareness-raising programmes should focus on mobile phones as opposed to laptops and iPads, as the majority of South Africans use mobile phones to access cyber space (literacy and education; inequality and poverty).

Relating to ***cyber safety***, citizens must be informed on how to deal with cyber bullying, stalking, identity theft and unwanted sexting. These topics must be included in primary and secondary school education and curriculums and can be incorporated in the proposals of the Department of Basic Education when designing the planned digital skills strategy for South Africa (BusinessTech, 2020).

On the issue of ***cyber security***, users must be educated about the use of anti-virus programs. That must include information on where to download such programs and how to use them. They must also be provided with information on the physical security of their devices and how to make backups. Finally, they must be told that current password “best practice” is now outdated. The latest “best practice” guidelines suggest that length, not complexity, ought to be maximised (Grassi et al., 2017; GOV.UK Design System, n.d.). The Cyber4Dev-Q must be updated to reflect this information, as should the training itself.

As to ***cyber privacy***, the focus must be on where website privacy and security policies can be found, what the policies typically cover and mean, and how the privacy settings of social media accounts can be changed. Privacy terms and conditions of mobile applications should also be addressed. This is particularly important as the South African data protection act, the *Protection of Personal Information Act* of 2013 (South African Government, 2013), came into force on 01 July 2020 and the grace period lapsed on 01 July 2021. This places a responsibility on the government and information regulator of South Africa to improve cyber privacy literacy and to conduct awareness to ensure that citizens are aware of their privacy rights. In this context, not only English but *all* local vernaculars must be included in campaigns. Existing infrastructure such as schools and church halls can be leveraged for dissemination of information and the preferred methods of communication can be integrated in the approach.

It is hoped that independent organisations can leverage the data gathered via the Cyber4Dev-Q to inform the content of their outreach programmes so that the focus can be on those areas of cyber safety, security and privacy that were highlighted as requiring more focused attention (Figure 6).

Figure *6*: Refinements of Security Training

6.2 Research implications

This study highlighted the importance of context in measuring cyber awareness. The context focused on was that of a developing country. Based on the understanding that there was no existing instrument tailored towards the measurement of cyber awareness in this context, the Cyber4Dev-Q was developed. Other researchers have developed questionnaires for country-specific studies, but those have generally only been used for particular studies in employee-organisational contexts. It is important for further research to be carried out in the following areas:

(1) Development of ways to feed a particular country's context-specific needs into the Cyber4Dev-Q. It is currently tailored to the needs of one specific country (South Africa). Because developing countries are not homogenous, it would be helpful if other countries could make use of it as well. To achieve this, it would be desirable to develop a question bank that could be mined to match the particular country context of a research study.

(2) Development of a mechanism for keeping the questionnaire current. This is important in the light of the fluidity and dynamism of the cyber domain. For example, in 2017 Grassi et al. published a new set of password guidelines. This challenged traditional guidelines in a number of areas, including the advisability of password expiration and password complexity requirements. Revisions to current survey instruments would have to be designed or they would risk becoming outdated while sub-optimal principles would be taught.

(3) Some computer users are particularly vulnerable in cyber space. These might be senior citizens, those with cognitive disabilities or those who do not understand English very well. Ways of meeting the cyber needs of such users should be studied (Renaud, 2021).

7. Limitations

The study was limited in that the Cyber4Dev-Q was validated in a single community in South Africa. During future research the Cyber4Dev-Q would be administered to other community groups across South Africa and in other African countries to develop more questions that could be used in a question bank. The Cyber4Dev-Q would be refined and improved using the factor and item analyses of this study. Because no survey instrument measures actual behaviours and the Cyber4Dev-Q does not offer the opportunity to confirm the veracity of responses, the aim is to conduct future interviews with developing country citizens in their home languages. That would facilitate richer data collection to inform cyber awareness and training programmes based on the outcome of the Cyber4Dev-Q in the local area.

8. Conclusion

The objective of this study was to develop a cyber awareness measurement instrument (Cyber4Dev-Q) that satisfied three requirements: It had to be (1) country context-sensitive; that is designed for a developing country context (the underserved, under-resourced, and under-represented), (2) comprehensive; that is including questions about all three cyber concepts (cyber safety, cyber security and cyber privacy), and (3) individual focused as opposed to targeting employees within organisations. The Cyber4Dev-Q was validated in an urban city in South Africa and revealed clear cyber awareness gaps that can inform future cyber awareness drives. The Cyber4Dev-Q is the first context-sensitive cyber awareness measurement instrument that accommodates the needs of developing country citizens. It is hoped that researchers will test this instrument in other developing countries and that a question bank can ultimately be developed for use in various developing country contexts. The aim of the researchers is to work towards a useful instrument that can benefit awareness drives across the developing world. A subset of the questions is provided in Table 3 and the final validated Cyber4Dev-Q is available as additional material.

Funding

National Research Foundation of South Africa: Grant number 103965.

Data Availability Statement

Data available on request due to privacy/ethical restrictions.

References

Akhter, M. S., Islam, M. H., and Momen, M. N. (2020). Problematic internet use among university students of Bangladesh: The predictive role of age, gender, and loneliness. *Journal of Human Behavior in the Social Environment*, *30*(8), 1082–1093. https://doi.org/10.1080/10911359.2020.1784346

Aldawood, H., and Skinner, G. (2018, December 4–7*). Educating and raising awareness on cyber security social engineering: a literature review*. In *IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, Wollongong, NSW, Australia, http://dx.doi.org/10.1109/TALE.2018.8615162

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Arde, A. (2014, October 6). Cellphone cover: The smart thing to do. *Independent Online*. https://www.iol.co.za/personal-finance/cellphone-cover-the-smart-thing-to-do-1759957

Bada, M., Von Solms, B., and Agrafiotis, I. (November 18–22). *Reviewing national cybersecurity awareness in Africa: an empirical study*. In Third International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2018), Athens, Greece. 78-83. https://www.repository.cam.ac.uk/handle/1810/293742

Balfour, C. (2005). *A journey of social change: Turning government digital strategy into cybersafe local school practices*. In International Conference on Cyber-Safety, Oxford University, Oxford, United Kingdom.

Balhara, Y. P. S., Harshwardhan, M., Kumar, R., and Singh, S. (2018). Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness programme. *Asian Journal of Psychiatry*, *34*, 38–42. https://doi.org/10.1016/j.ajp.2018.04.010

Banciu, D., Rădoi, M., and Belloiu, S. (2020). Information security awareness in Romanian public administration: An exploratory case study. *Studies in Informatics and Control*, *29*(1), 121–129. https://doi.org/10.24846/v29i1y202012

Bartlett, J. E., Kotrlik, J., and Higgins, C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal, 19*(1), 43–50.

Beach, R. (2007). *New Zealand's first steps to cybersafety*. In proceedings of Early Childhood Convention, Rotorua, New Zealand.

Benson, V., Saridakis, G., and Tennakoon, H. (2015). Information disclosure of social media users. *Information Technology and People*, *28*(3), 426–441. https://doi.org/10.1108/ITP-10-2014-0232

Blue Turtle Technologies. (2020). *Cyber Crime a pandemic hitting the wallet of South African business*. https://www.itweb.co.za/content/JN1gPvOYBWPMjL6maa

Brewerton, P. M., and Millward, L. J. (2001). *Organizational research methods: A guide for students and researchers*. Sage.

BusinessTech. (2020, September 23). *These are the skills government wants South African schools to cover*. https://businesstech.co.za/news/technology/435649/these-are-the-skills-government-wants-south-african-schools-to-cover/

Calandro, E., and Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace

Governance: The SADC case. https://researchictafrica.net/wp/wp-content/uploads/2020/07/GIGAnet-presentation-v02.pdf

Cindana, A., and Ruldeviyani, Y. (2018). Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firm. In *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 289–294. IEEE. https://doi.org/10.1109/ICACSIS.2018.8618219

City of Tshwane. (2014). *Region 3: Regional Integrated Development Plan, 2014/15*. http://www.tshwane.gov.za/sites/Council/Ofiice-Of-The-Executive-Mayor/20162017%20IDP/Annexure%20D%20Region%203%20RIDPv9_090514.pdf

City of Tshwane. (2020). *Welcome to free TshWi-Fi by the City of Tshwane*. http://www.tshwane.gov.za/Pages/WIFI.aspx.

Craigen, D., Diakun-Thibault, N., and Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. http://doi.org/10.22215/timreview/835

Creswell, J. W., and Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Cyber4Dev. (n.d.). *We are Cyber 4*. https://cyber4dev.eu/

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture*. Information & Computer Security*, *26(*5), 584–612. https://doi.org/10.1108/ICS-08-2017-0056

Dharmawansa, A. D., and Madhuwanthi, R. A. M. (2020, October 15). *Evaluating the information security awareness (ISA) of employees in the banking sector: a case study*. In proceedings 13th International Research Conference, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka, 147-154, KDUIRC. http://ir.kdu.ac.lk/bitstream/handle/345/2844/pdfresizer.com-pdf-split%20%283%29.pdf?sequence=1&isAllowed=y

Egelman, S., Harbach, M., and Peer, E. (2016). Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '16)* 5257–5261. ACM https://blues.cs.berkeley.edu/wp-content/uploads/2016/02/article1.pdf

Elgot, J. (2015, September 22). One in five young people has suffered online abuse, study finds. *The Guardian*. https://www.theguardian.com/society/2015/sep/22/cyberbullying-teenagers-worse- than-drug-abuse-says-report

Elradi, M. D., Altigani, A., and Abaker, O. I. (2020). Cyber security awareness among students and faculty members in a Sudanese college. *Electrical Science & Engineering*, *2*(2), 24–28. https://doi.org/10.30564/ese.v2i2.2477

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., & Maglaras, L. A. (2019). Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form. *IEEE Access*, *7*, 102087–102101. https://doi.org/10.1109/ACCESS.2019.2927195

Frechette, J. (2005). Cyber-democracy or cyber-hegemony? Exploring the political and economic structures of the Internet as an alternative source of information. *Library Trends*, *53*(4), 555–575. http://hdl.handle.net/2142/1748

Funke, D., and Flamini, D. (2021, July 6). A guide to anti-misinformation actions around the world. *Poynter.* https://www.poynter.org/ifcn/anti-misinformation-actions/

Gerber, H., and Hall, R. (2017). Quantitative research design [Workshop handout]. HR Statistics (Pty) Ltd, South Africa.

Ginosar, A., and Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, *54*(7), 948–957. https://doi.org/10.1016/j.im.2017.02.004

Global Action on Cybercrime. (n.d.). Strategic priorities for cooperation on cybercrime and e-evidence in GLACY countries. https://www.coe.int/en/web/cybercrime/glacy

Global Forum on Cyber Expertise. (2019). Cybercrime Model Laws. Discussion paper prepared for the Cybercrime Convention Committee, 1–5 September.

GOV.UK. (2020). *Cyber Security Breaches Survey 2020*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

GOV.UK Design System. (n.d). *Ask users for passwords*. https://design-system.service.gov.uk/patterns/passwords/

Grassegger, T., and Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y-Y., Greene, K. K., and Theofanos, M. F. (2017). NIST Special Publication 800-63B, Digital Identity Guidelines. https://doi.org/10.6028/NIST.SP.800-63b

Grey, A. (2011). Cybersafety in early childhood education. *Australasian Journal of Early Childhood*, *36*(2), 77–

81. https://doi.org/10.1177%2F183693911103600210

Grobler, M., Dlamini, Z., Ngobeni, S., and Labuschagne, A. (2011). Towards a cyber security aware rural community. In Proceedings of the 2011 Information Security for South Africa (ISSA) Conference, Hayatt Regency Hotel, Rosebank, Johannesburg, South Africa 15 - 17 August 2011. http://hdl.handle.net/10204/5183

Grobler, M., Jansen Van Vuuren, J. J., and Leenen, L. (2012). Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. In Hercheui, M. D., Whitehouse D., McIver, W., Phahlamohlaka, J. (Eds.), *ICT Critical Infrastructures and Society*. *HCC 2012. IFIP Advances in Information and Communication Technology*, *386*, 215–225, Springer. https://doi.org/10.1007/978-3-642-33332-3_20

Gundu, T., Flowerday, S. and Renaud, K. (2019). Deliver security awareness training, then repeat: {Deliver; Measure Efficacy}. *2019 Conference on Information Communications Technology and Society (ICTAS)* 1–6. IEEE. http://dx.doi.org/10.1109/ICTAS.2019.8703523

Hadlington, L., Binder, J., & Stanulewicz, N. (2020). Fear of missing out predicts employee information security awareness above personality traits, age, and gender. *Cyberpsychology, Behavior, and Social Networking*, *23*(7), 459–464. https://doi.org/10.1089/cyber.2019.0703

Hagen J. M., Albrechtsen, E., and Hovden, J. (2008) Implementation and effectiveness of organizational information security measures. *Information Management and Computer Security*, *16*(4), 377–397. http://dx.doi.org/10.1108/09685220810908796

Hayden, L. (2015). *People-centric security: Transforming your enterprise security culture*. McGraw Hill Professional, New York, USA.

IBM Security. (2020). *Cost of data breach report*. https://www.ibm.com/security/data-breach

International Telecommunication Union. (2014). *LDCs Infrastructure Protection Program: Comoros. 1–5 September.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/LDC_Comoros.aspx

International Telecommunication Union. (2021). *National Cybersecurity Strategies Repository*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Jamil, Z. (2014). Cybercrime model laws [Discussion paper]. https://rm.coe.int/1680303ee1

Kahla, C. (2020, September 24). SA, Kenya and Nigeria report highest cyber attacks in Africa. *The South African*. https://www.thesouthafrican.com/technology/cyber-security-south-africa-kenya-nigeria/

Kaiser, H. F., and Rice, J. (1974). Little jiffy, mark IV. *Educational and Psychological Measurement*, *34*(1), 111–

117. https://doi.org/10.1177%2F001316447403400115

Kandri, S. E. (2019, October 23). Africa’s future is bright—and digital. *World Bank Blogs*. https://blogs.worldbank.org/digital-development/africas-future-bright-and-digital

Kortjan, N., & Von Solms, R. (2013) Cyber security education in developing countries: A South African perspective. In Jonas, K., Rai, I. A., Tchuente, M. (Eds.). *e-Infrastructure and e-Services for Developing Countries,* 289–297. Springer. https://doi.org/10.1007/978-3-642-41178-6_30

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, *29*(2), 16–35. http://dx.doi.org/10.18489/sacj.v29i2.471

Kritzinger, E., Bada, M., & Nurse, J. R. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In Bishop, M., Futcher, L., Miloslavskaya, N., Theocharidou (Eds.). *Information Security Education for a Global Digital Society,* 110–120. Springer. https://doi.org/10.1007/978-3-319-58553-6_10

Kruger, H. A., and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. http://dx.doi.org/10.1016/j.cose.2006.02.008

Lamp, J. W. (2017). Preface to Selected Papers from ACIS 2016. *Australasian Journal of Information Systems*, *21*. https://doi.org/10.3127/ajis.v21i0.1715

Lewis, M. (2020, September 22). Game or shame - how to teach employees to be cybersecurity aware. *MOBILECORP*. https://www.mobilecorp.com.au/blog/game-or-shame-how-to-teach-employees-to-be-cybersecurity-aware

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Talking to children about data and privacy online: research methodology. London: London School of Economics and Political Science. http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Talking-to-children-about-data-and-privacy-online-methodology-final.pdf

Makoni, M. (2020, October 8). Cyberattack surge highlights Africa security risk. *SciDevNet.* https://www.scidev.net/sub-saharan-africa/news/cyberattack-surge-highlights-africa-security-risk

McDowell, M. (2010, October 12). Language challenges in South Africa. *Connect-123*. https://www. connect-123.com/language-challenges-in-south-africa/

Nagyfejeo, E., and Von Solms, B. (2020). Why do national cybersecurity awareness programmes often fail? *International Journal of Information Security and Cybercrime*, *9*(2):18–27. https://www.ijisc.com/year-2020-issue-2-article-3/

Naik, S. (2021, March 27). SA youngsters under threat from cyber bullies as online shaming and revenge porn also on the rise. *IOL*. https://www.iol.co.za/saturday-star/news/sa-youngsters-under-threat-from-cyber-bullies-as-online-shaming-and-revenge-porn-also-on-the-rise-e6f391d5-0be6-4b52-881c-d929964122da

Ndou, V. (2004). E–Government for developing countries: Opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, *18*(1): 1–24. https://doi.org/10.1002/j.1681-4835.2004.tb00117.x

Nhlapo, Z. (2017, October 27). Sexting – The Shocking Pandemic among South African Teens. *HUFFPOST*. https://www.huffingtonpost.co.uk/2017/10/27/sexting-the-shocking-pandemic-among- south-african-teens_a_23257928/

Nilsen, R. (2017). Measuring cybersecurity competency: An exploratory investigation of the cybersecurity knowledge, skills, and abilities necessary for organizational network access privileges [Doctoral dissertation]. Nova Southeastern University. https://nsuworks.nova.edu/gscis_etd/1017

9 major problems facing South Africa - and how to fix them. (2011, July 18). *Leader.* http://www.leader.co.za/article.aspx?s=1&a=2893

Oates, B.J. (2005). *Researching information systems and computing*. Sage, London, UK.

Oliver Wyman Forum. (2021*). Cyber Risk Literacy and Education Index*. https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html

O'Rourke, N., and Hatcher, L. (2013). *A step-by-step approach to using SAS for factor analysis and structural equation modelling* (2nd ed.). SAS Institute.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. http://dx.doi.org/10.1016/j.cose.2013.12.003

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*:40–51. https://doi.org/10.1016/j.cose.2017.01.004

Ponemon Institute. (2017). *Cost of data breach study*. https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.

Popovac, M., and Leoschut, L. (2012). Cyber bullying in South Africa: Impact and responses [Issue paper No. 13]. Centre for Justice and Crime Prevention.

http://www.cjcp.org.za/uploads/2/7/8/4/27845461/issuepaper13-cyberbullying-sa-impact_responses.pdf

Renaud, K. (2021). Accessible Cyber Security: The Next Frontier? *In Proceedings of the 7th International Conference on Information Systems Security and Privacy*, 9–18. doi.10.5220/0010419500090018

Saridewi, V. S., and Sari, R. F. (2020). Feature selection in the human aspect of information security questionnaires using multicluster feature selection. *International Journal of Advanced Science and Technology*, *29*(7 Special Issue), 3484–3493.

Saunders, M., Lewis, P., and Thornhill, A. (2009). *Research methods for business students* (5th ed.). Pearson Education, Harlow, UK.

Schlienger, T., and Teufel, S. (2005). Tool supported management of information security culture. In Sasaki R., Qing S., Okamoto E., Yoshiura H. (Eds.). *Security and Privacy in the Age of Ubiquitous Computing. SEC 2005. IFIP Advances in Information and Communication Technology, 181*, 65-77 Springer. https://doi.org/10.1007/0-387-25660-1_5

Security Awareness Company. (2017). *Cyber security risks on social media: 5 ways users are vulnerable*. https://www.thesecurityawarenesscompany.com/2017/06/06/cyber- security-risks-social-media-5-ways-users-vulnerable/

Sihlangu, J. (2019, September 25). Identity fraud and theft on the rise in South Africa compared to 2018. *The South African*. https://www.thesouthafrican.com/news/finance/increase-identity-fraud-and-theft- in-south-africa/

Sissing, S. K. (2013). A criminological exploration of cyber stalking in South Africa [Master’s thesis]. University of South Africa, Pretoria. http://hdl.handle.net/10500/13067

South African Cyber Security Academic Alliance. (n.d). *Cyber Security Awareness Workbook* http://eagle.unisa.ac.za/elmarie/images/Pdf/book.pdf

South African Government (2013). *Protection of Personal Information Act 4 of 2013. Government Gazette No. 37067*, 1–76. Government Printing Works. https://www.gov.za/documents/protection-personal-information-act

Statista. (2020). *Number of smartphone users in South Africa from 2014 to 2023*. https://www.statista.com/statistics/488376/forecast-of-smartphone-users-in-south-africa/

Statistics South Africa. (2011). *Census 2011. Region 3: Regional Integrated Development Plan, 2014/15.* http://www.statssa.gov.za/?page_id=4286&id=11387

Statistics South Africa. (2019). *Unemployment raises slightly in third quarter in 2019*.

http://www.statssa.gov.za/?s=unemployment+rate&sitem=content.

Statistics South Africa. (2020). *Census 2001*. http://www.statssa.gov.za/census/census_2001/urban_rural/urbanrural.pdf.

Surbhi, S. (2020, April 17). Difference between developed countries and developing countries. *Key Differences*. https://keydifferences.com/difference-between-developed-countries-and- developing-countries.html

Sutherland, E. (2017). Governance of cybersecurity - The case of South Africa. *The African Journal of Information and Communication*, *20*(20), 83–112. http://dx.doi.org/10.23962/10539/23574

Trading Economics. (2021). *South Africa Unemployment Rate*. https://tradingeconomics.com/south-africa/unemployment-rate.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*, *17*, 207–227. https://doi.org/10.1080/19393550802492487

Öłütçü, G., Testik, Ö. M., and Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Unwin, T. (Ed). (2009). *ICT4D Information and Communication Technologies for Development*. Cambridge University Press, Cambridge, UK.

Van der Spuy, A. (2018). Collaborative Cybersecurity: The Mauritius Case. (Policy Brief No. 1; Africa Digital Policy). Research ICT Africa. https://researchictafrica.net/wp/wp- content/uploads/2018/11/Policy-Brief-ADPP-N-1-Collaborative-Cybersecurity-Mauritius- Case.pdf

Velki, T., and Šolić, K. (2019). Development and validation of a new measurement instrument: The behavioral-cognitive internet security questionnaire (BCISQ). *International Journal of Electrical and Computer Engineering Systems*, *10*, 19–24. http://dx.doi.org/10.32985/ijeces.10.1.3

Velki, T., Šolić, K., Očevćić, H. (2014). Development of users' information security awareness questionnaire (UISAQ) - ongoing work. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1417–1421. IEEE.

Venter, I. M., Blignaut, R. J., Renaud, K., and Venter, M. A. (2019). Cyber security education is as essential as "The three R's". *Heliyon*, 5(12), e02855.

Wahyudiwan, D. D. H., Sucahyo, Y. G., and Gandhi, A. (2017, October). Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 654–658. IEEE.

Walker, A. (2020). Phishing and malware attacks rise as SA goes into COVID-19 lockdown. *MEMEBURN.* https://memeburn.com/2020/03/cyber-attacks-south-africa-lockdown/

Wang, Y., Qi, B., Zou, H. X., and Li, J. X. (2018). Framework of raising cyber security awareness. In *IEEE 18th International Conference on Communication Technology (ICCT)*, 865–869. IEEE. https://doi.org/10.1109/ICCT.2018.8599967

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166–170. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

Wilby, M. (2010). The simplicity of mutual knowledge. *Philosophical Explorations*, *13*(2), 83–100. https://philpapers.org/go.pl?id=WILTSO-7&proxyId=&u=http%3A%2F%2Fdx.doi.org%2F10.1080%2F13869791003759963

Wild, S. (2020, March 04). Citing virus misinformation, South Africa tests speech limits. *UNDARK.* https://undark.org/2020/04/03/fake-news-south-africa-covid-19/

Wolf, M., Haworth, D. A., & Pietron, L. (2011). Measuring an information security awareness program. *Review of Business Information Systems*, *15*(3), 9–21. https://doi.org/10.19030/rbis.v15i3.5398

Wolfpack Information Risk. (2018). *Cybercrime survival guide*. https://www.wits.ac.za/media/wits-university/news-and-events/images/documents/2020/Cybercrime%20Survival%20Guide.pdf

Zulfia, A., Adawiyah, R., Hidayanto, A. N., and Budi, N. F. A. (2019, April). Measurement of employee information security awareness using the human aspects of information security questionnaire (HAIS-Q): Case study at PT. PQS. In *2019 5th International Conference on Computing Engineering and Design (ICCED),* 1–5. IEEE. https://doi.org/10.1109/ICCED46541.2019.9161120

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., and Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1–16. https://doi.org/10.1080/08874417.2020.1712269

Appendix A

Table 4: The Cyber Awareness Calibration Instrument for Developing Countries (Cyber4Dev-Q) – initially proposed Themes and Items (sec=security, saf=safety, priv=privacy)

Table 5: The Cyber Awareness Calibration Instrument for Developing Countries (Cyber4Dev-Q) – Results of Analysis

Additional material

Questionnaire

Figure Legend

Figure 7: Cyber Awareness Raising Stages

Figure 8: Dimensions of the three related cyber concepts

Figure 9: South Africa’s Challenges (Map by Allice Hunter from: https://commons.wikimedia.org/wiki/File:South_African_provinces_by_HDI_(2017).svg)

Figure 10: Allocation of questions to Cyber Concepts and co-dependencies

Figure 11: Word clouds with usage of devices

Figure 12: Refinements of Security Training

Table Caption

Table 6: Existing Cyber Awareness Measurement Instruments (•=satisfies; Ø=fails)

Table 7: Demographics of Respondents participating in the Chance2Advance Event hosted in Atteridgeville

Table 8: New Factors and Cronbach’s Alpha Values

Table 9: The Cyber Awareness Calibration Instrument for Developing Countries (Cyber4Dev-Q) – Initially proposed Themes and Items (sec=security, saf=safety, priv=privacy)

Table 10: The Cyber Awareness Calibration Instrument for Developing Countries (Cyber4Dev-Q) – Results of Analysis

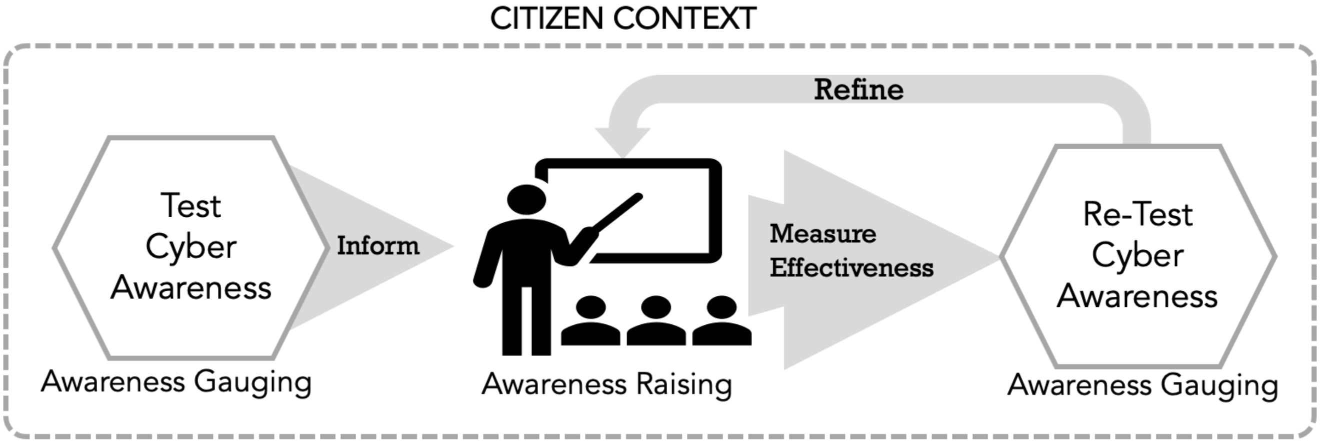


Figure 13: Cyber Awareness Raising Stages

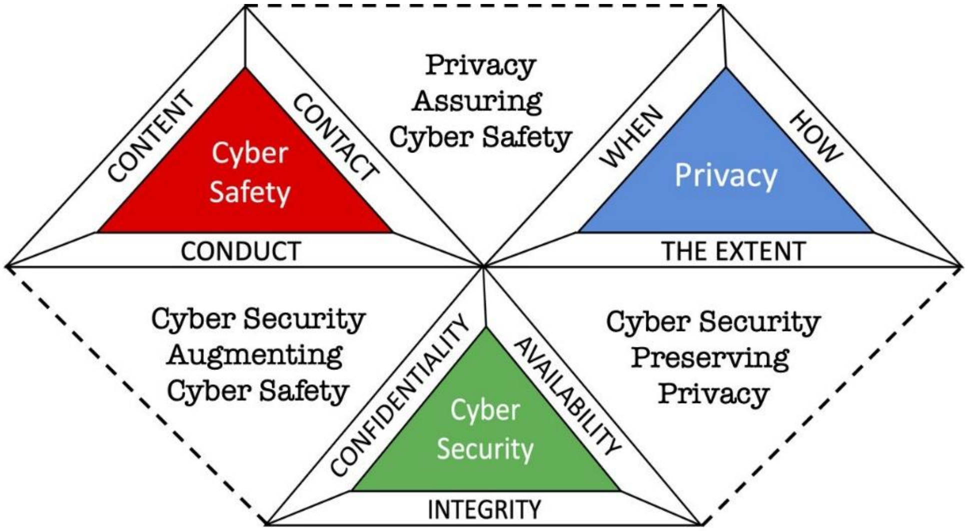


Figure 14: Dimensions of the three related cyber concepts

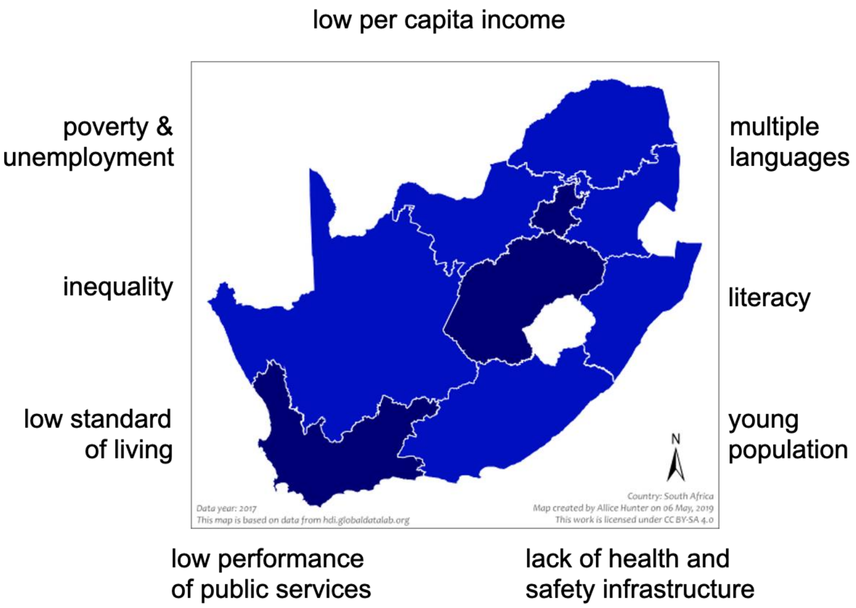
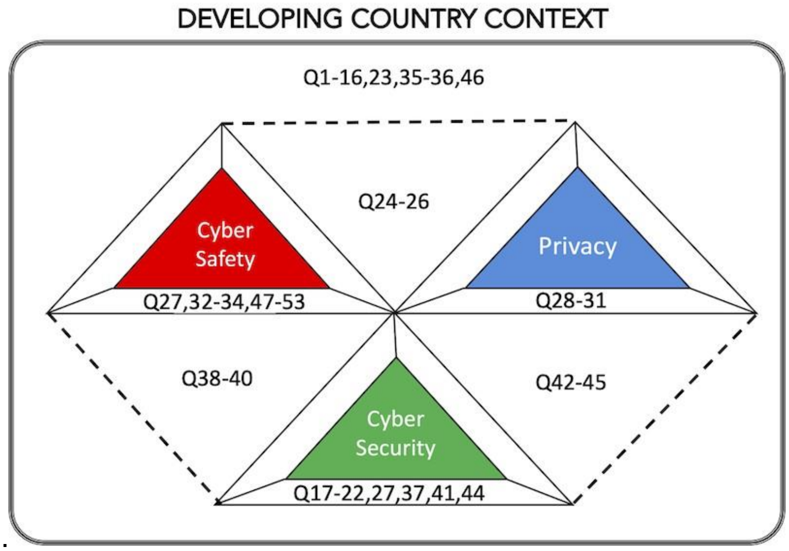

low per capita income
poverty & unemployment
inequality
low standard of living
multiple languages
literacy
young population
low performance of public services
lack of health and safety infrastructure
N
Data year: 2017
This map is based on data from hdi.globaldatalab.org
Country: South Africa
Map created by Allice Hunter on 06 May, 2019
This work is licensed under CC BY-SA 4.0

Figure 15: South Africa's Challenges (Map by Allice Hunter from: https://commons.wikimedia.org/wiki/File:South_African_provinces_by_HDI_(2017).svg)



.

Figure *16*: Allocation of questions to Cyber Concepts and co-dependencies

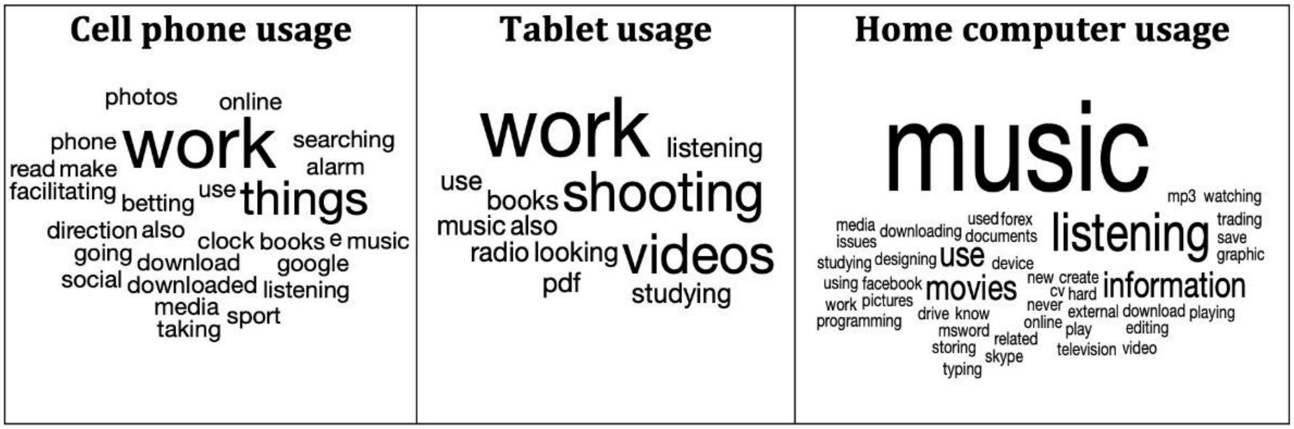


Figure *17*: Word clouds with usage of devices

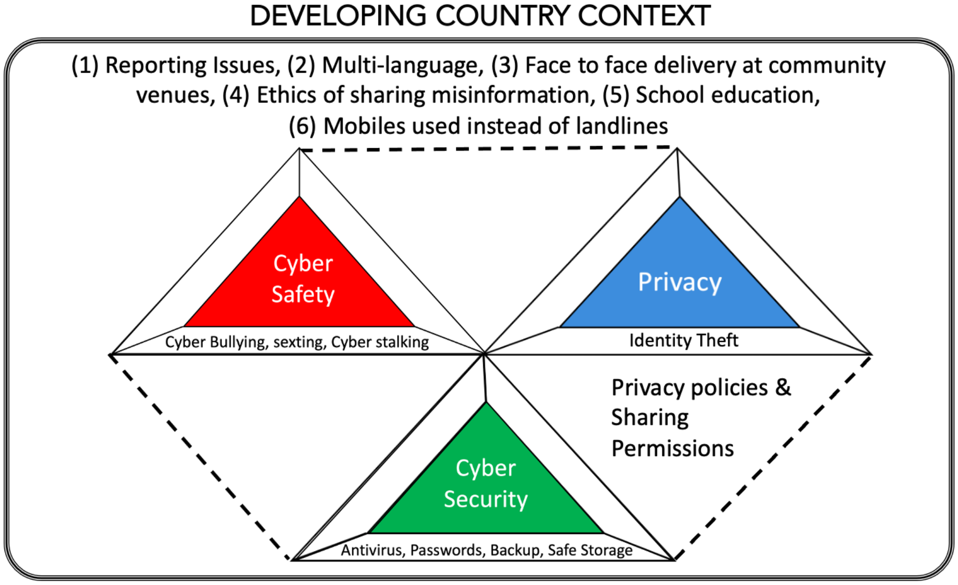

DEVELOPING COUNTRY CONTEXT
(1) Reporting Issues, (2) Multi-language, (3) Face to face delivery at community venues, (4) Ethics of sharing misinformation, (5) School education, (6) Mobiles used instead of landlines
Cyber Safety
Cyber Bullying, sexting, Cyber stalking
Privacy
Identity Theft
Privacy policies & Sharing Permissions
Cyber Security
Antivirus, Passwords, Backup, Safe Storage

Figure *18*: Refinements of Security Training

Table 11: Existing Cyber Awareness Measurement Instruments (•=satisfies; Ø=fails)

Reference	Description	Comprehensiveness	Individual focus (not workplace)	Country context-sensitive	Country
Kruger & Kearney, 2006	Security awareness program for organisations	•	Ø	Ø	Australia
Hagen et al., 2008	Organisational security measures questionnaire	Cyber safety and cyber privacy excluded	Ø	Ø	Norway
Velki et al., 2014	Users' information security awareness questionnaire	Cyber safety and cyber privacy excluded	•	Ø	Croatia
Öłütçü et al., 2016	Four scales: risky behavior scale (RBS), conservative behavior scale (CBS), exposure to offence scale (EOS) and risk perception scale (RPS)	Cyber safety excluded	Ø	Ø	Turkey
Velki & Šolić, 2019	Behavioural-cognitive internet security questionnaire	Cyber safety and cyber privacy excluded	•	Ø	Croatia
Egelman et al., 2016	Security behavior intentions scale (SeBIS)	Cyber safety excluded	•	Ø	USA
Parsons et al., 2017	HAIS-Q for employers	Cyber safety cyber security	Ø	Ø	Australia
Wahyudiwan et al., 2017	Knowledge, attitude and behavior model (KAB) for organisations	Cyber safety and cyber privacy excluded	Ø	Ø	Indonesia
Balhara et al., 2018	Generalised problematic internet use (PIU) scale 2	Cyber safety only		Ø	India
Nilsen, 2017	MyCyberKSAs™ prototype tool, organisational awareness	Cyber security only	Ø	Ø	USA
Akhter et al., 2020	PIU, IDS9-SF	Cyber safety only	•	•	Bangladesh
Banciu et al., 2020	Based on ISO 27001	Cyber safety excluded	Ø	•	Romania
Zwilling et al., 2020	Explores links between cyber security awareness, knowledge and behaviour	Cyber security only	•	•	Israel, Slovenia, Poland and Turkey
Elradi et al., 2020	Cyber security awareness	Cyber security only	•	•	Sudan
Evans et al., 2019	Information security core human error causes (IS-CHEC) technique,	Cyber security only	Ø	Ø	United Kingdom

Reference	Description	Comprehensiveness	Individual focus (not workplace)	Country context-sensitive	Country
	human reliability analysis (HRA)				
Grassegger & Nedbal, 2021	Security awareness program for organisations	Cyber security only	Ø	•	Austria
Alzubaidi, 2021	Measuring security awareness of cyber crime	Cyber security only	•	•	Saudi Arabia

Table 12: Demographics of Respondents participating in the Chance2Advance Event hosted in Atteridgeville

First language	N	% of total	Qualification	N	% of total
Xhosa	1	0.68	Below Grade 12	36	24.00
Zulu	13	8.84	Grade 12/Matric	94	62.67
English	11	7.48	Diploma	7	4.67
Ndebele	5	3.40	Three-year university degree	6	4.00
Northern Sotho	47	31.97	Honours	0	0.00
Sotho	26	17.69	Master’s degree	1	0.67
Swazi	1	0.68	None	6	4.00
Tsonga	9	6.12			
Tswana	18	12.24			
Venda	7	4.76			
Sepedi or Pedi	9	6.12			
Year of birth	**N**	**% of total**	**Employment status**	**N**	**% of total**
1946–1954	1	0.69	Employed	26	17.69
1955–1964	3	2.08	Student	21	14.29
1965–1980	34	23.61	Unemployed	98	66.67
1981–2000	106	73.61	Retired	2	1.36

Table 13: New Factors and Cronbach's Alpha Values

Factors	New factor names	Question numbers	Total items	Cronbach's alpha
F1	Cyber safety and privacy risk awareness	Q38, Q39, Q40, Q41, Q42, Q43, Q44, Q45, Q46 , Q47, Q48, Q49, Q50	13	0.899
F2	Cyber security protection	Q17, Q18, Q19, Q20	4	0.859
F3	Personal cyber safety	Q30, Q31, Q32, Q34, Q36	5	0.682
F4	Cyber safety risks	Q51, Q52	2	0.813
F5	Cyber privacy actions	Q24, Q25, Q26	3	0.745
F6	Cyber security for passwords	Q21, Q22	2	0.682

Table 14: The Cyber Awareness Calibration Instrument for Developing Countries (Cyber4Dev-Q) – Initially proposed Themes and Items (sec=security, saf=safety, priv=privacy)

Context		Cyber topic		
Section 2.3 Challenge	**Item to include in questionnaire**	**Sec**	**Saf**	**Priv**
PRIVACY				
	Selective sharing of personal information (Wolfpack Information Risk, 2012)			•
Literacy and educational	Changing of default privacy settings (Parsons et al., 2017; Wolfpack Information Risk, 2012)			•
Literacy and educational	Awareness of website privacy policy (Ginosar & Ariel, 2017; Benson et al., 2015)			•
Literacy	Reading of website privacy policies (Ginosar & Ariel, 2017; Benson et al., 2015)			•
Literacy and educational	Understanding of website privacy policies (Ginosar & Ariel, 2017)			•
CYBER SAFETY				
Educational	Being victimised in cyberspace (SACSAA, 2020; Wolfpack Information Risk, 2012; Elgot, 2015)		•	
	Adding known friends to social networks (SACSAA, 2020; Wolfpack Information Risk, 2012)		•	
	Perceptions about the possibility of cyber stalking (SACSAA, 2020; Wolfpack Information Risk, 2012; Sissing, 2013)		•	
	Perceptions about the possibility of cyber bullying		•	

Context		Cyber topic		
Section 2.3 Challenge	Item to include in questionnaire	Sec	Saf	Priv
	(SACSAA, 2020; Naik, 2021; Elgot, 2015; Popovac & Leoschut, 2012)			
	Perceptions about cases of cyber bullying (SACSAA, 2020; Naik, 2021; Elgot, 2015; Popovac & Leoschut, 2012)		•	
Educational	Experience of sexting (Kritzinger, 2017; Nhlapo, 2017)		•	
	Perceptions about friends experiencing sexting (Kritzinger, 2017; Nhlapo, 2017)		•	
CYBER SECURITY				
Infrastructure	Backing up of information (Egelman et al., 2016; SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Literacy and educational	Understanding of anti-virus software(SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Basic principles	Having anti-virus software installed (Egelman et al., 2016; SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
	Knowing what a personal firewall is (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
	Having a personal firewall installed (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Literacy	Using a password on devices (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Literacy	Using strong passwords (Parsons et al., 2017; SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Inequality and low standard of living	Choosing a physically-safe location for electronic device storage (Wolfpack Information Risk, 2012)	•		
	Perception that information on lost devices can be used for criminal purposes (Wolfpack Information Risk, 2012; Africa Check, 2020; Arde, 2014)	•		
	Perceptions about back-ups	•		

Context		Cyber topic		
Section 2.3 Challenge	Item to include in questionnaire	Sec	Saf	Priv
	(SACSAA, 2020)			
Literacy and low per capita income	Perceptions about banking credentials being stolen in cyber space (SACSAA, 2020)	•		
	Perceptions about phishing (responding to unknown e-mails) (SACSAA, 2020; Wolfpack Information Risk, 2012; Walker, 2020)	•		
	Perceptions that devices can become infected (SACSAA, 2020; Wolfpack Information Risk, 2012; Kahla, 2020)	•		
	Perceptions that devices can be implicated in crimes (Wolfpack Information Risk, 2012; Africa Check, 2020)	•		
	Perceptions that criminals can access devices (Wolfpack Information Risk, 2012)	•		
PRIVACY & CYBER SECURITY				
	Perceptions about identity theft (SACSAA, 2020; Wolfpack Information Risk, 2012; Sihlangu, 2019)	•		•
	Perceptions about personal information stolen in cyber space (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		•
CYBER SAFETY & CYBER SECURITY				
Public service issues	Awareness of reporting cyber incidents (SACSAA, 2020; Wolfpack Information Risk, 2012)	•	•	
Public service issues	Effectiveness of reporting (SACSAA, 2020; Wolfpack Information Risk, 2012)	•	•	
	Responding to unwanted messages (Egelman et al., 2016; SACSAA, 2020; Wolfpack Information Risk, 2012; Parsons et al., 2017)	•	•	
Different country approaches	Perceptions about posting inaccurate information (SACSAA, 2020; Wild, 2020; Funke & Flamini, 2018)	•	•	

Table 15: The Cyber Awareness Calibration Instrument for Developing Countries (Cyber4Dev-Q) – Results of Analysis

Statements	New factors
Q17. I know what an anti-virus software program is.	F2
Q18. I have an anti-virus software program installed on the computer I use.	F2
Q19. I know what a personal firewall program is.	F2
Q20. I have a personal firewall program installed on the computer that I use.	F2
Q21. I use a password on all my devices.	F6
Q22. My passwords consist of upper case, lower case, special characters and	F6
Q23. I have access to a safe place to lock away my electronic devices such as a phone or laptop.	Removed, <0.4, Move to Yes/No
Q24. I do not give out my personal information (like real name, age, location, etc.) when using online gaming applications.	F5
Q25. I do not post information (e.g. messages or photos) about my friends.	F5
Q26. I do not respond to unwanted communication or messages from people I do not know (like e-mails, WhatsApp, Facebook messages, etc.).	F5
Q27. I have a backup of information on my laptop or tablet that I can use if my laptop or tablet is stolen or broken.	Removed, cross loading, move to Yes/No
Q28. I changed the default privacy settings of my social media accounts.	
Q29. I know where to find a website's policy which explains how the website will protect my information.	
Q30. I read website policies relating to how my information is protected (e.g. privacy policy, security policy or terms and conditions) on websites.	F3
Q31. I understand website policies relating to how my information is protected (e.g. privacy policy, security policy or terms and conditions) on websites.	F3
Q32. I have NEVER been victimised in cyberspace (e.g. via social media like Facebook, Twitter or WhatsApp).	F3
Q33. I feel comfortable telling someone if something made me feel uncomfortable while using cyber space (e.g. Facebook, Twitter, WhatsApp, SMS, etc.).	Removed, <0.4 Move to Yes/No
Q34. I only add friends to my social networking profile if I know them.	F3
Q35. I know where to report a cyber security incident or crime.	Removed, <0.4, Move to Yes/No
Q36. No one that I know has ever experienced difficulty in reporting when they are victimised/harassed/bullied via a mobile phone or social media.	F3

Statements	New factors
Q37. I believe that a device like a laptop, mobile phone or tablet can become infected with viruses (malware).	Removed, cross loading, move to Yes/No
Q38. I believe that it is possible that my device can be implicated in cyber crime (this means, it looks as though the crime was committed using my device).	F1
Q39. I believe that criminals can access one's device (e.g. laptop, tablet) and the information on it through cyber space without physically having access to my device.	F1
Q40. I believe that if a device is lost or stolen the information could be used for criminal purposes.	F1
Q41. I believe it is important to back up information that is on my devices.	F1
Q42. I believe it is possible that one's identity can be stolen in cyber space.	F1
Q43. I believe it is possible that one's personal information can be stolen in cyber space, e.g. while playing online games or when using some apps.	F1
Q44. I believe that it is possible that one's bank accounts could be compromised and money stolen in cyber space.	F1
Q45. I believe there is risk in providing my personal information through an e-mail in response to an e-mail from an unknown entity.	F1
Q46. I (or my friends) believe it is unacceptable to post or share inaccurate or incorrect information in cyber space.	F1
Q47. I am aware that I can be stalked (e.g. online predators, harassment, unwanted communication) in cyber space.	F1
Q48. I believe my friends are aware that they can be stalked (e.g. online predators, harassment, unwanted communication) via an electronic device.	F1
Q49. I believe that I can be bullied in cyber space (e.g. via social media).	F1
Q50. I believe some of my friends have experienced cyber bullying (via an electronic device).	F1
Q51. I have experienced unwanted sexting in cyber space (e.g. via WhatsApp or Facebook).	F4
Q52. I believe some of my friends have experienced unwanted sexting in cyber space (e.g. via WhatsApp or Facebook).	F4
Q53. I believe I am safe in cyber space when doing anything that I want, as long as I stay anonymous or use a fake name.	Removed, <0.4, Move to Yes/No