Cyber4Dev-Q: Calibrating Cyber Awareness in the Developing Country Context

Adele Da Veiga[1], Mariaane Loock[1], Karen Renaud[1,2,3]
[1] University of South Africa, South Africa
[2] University of Strathclyde, UK
[3] Rhodes University, South Africa

Abstract

Citizens of the hyper-connected world face tremendous challenges in managing their personal online risks: preserving their cyber safety, cyber security and cyber privacy. Governments allocate significant resources to raising the awareness of their citizens in these three areas, to equip them to manage their online risks. To ensure maximum efficacy, these endeavours need to be able to gauge existing levels of awareness to ensure that awareness 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 terms of 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, which has been designed for this context, has a better chance of revealing particular awareness aspects requiring attention. To meet this need, we developed and validated a Cyber Awareness Questionnaire for use in developing countries (Cyber4Dev-Q), which aims to measure the cyber awareness of developing country citizens in all three core cyber areas in a context-sensitive fashion.

1 Introduction

Citizen cyber safety, security and privacy are a global concern for governments, organisations and individuals (GOV.UK, 2020; Blue Turtle Technologies, 2020; Security Awareness Company, 2017; Oliver Wyman, 2021). Governments across the world have formulated cyber security strategies to address the risks in cyberspace at national levels (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 and von Solms, 2012). This reality has led to a widely acknowledged need to improve global citizen cyber awareness.

Developing country citizens face particular challenges, which will impact on their general cyber awareness, as compared to developed country citizens. Ndou (2004) enumerates a number of these with the following being relevant for cyber awareness too: the general IT infrastructure of the country, human capital development and legislative issues. The Cyber for Development (Cyber4Dev) field emerged relatively recently to accommodate the needs of developing country citizens, with respect 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 developing country citizens are different from the needs of those residing in developed countries. Cyber4Dev researchers strive to acknowledge and accommodate the needs of *under-served under-resourced*, and *under-represented* global citizens (Unwin and Unwin, 2009).

In designing awareness raising interventions, we have to acknowledge that those living in developing countries have varied and different cyber-related needs, depending on their country's idiosyncrasies and level of development (Grobler et al., 2011). With respect to raising cyber awareness, focusing solely on the individuals without giving due consideration to their context would be naïve.

Indeed, Masha Sedova, co-founder of Elevate Security, argues that a one-size-fits-all approach to cyber training is bound to be ineffective (quoted by Lewis (2020)). It is unlikely that existing awareness levels can be accurately measured 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 is thus to develop a context-sensitive cyber awareness measurement instrument that can measure cyber awareness in the developing country context by accommodating the needs of developing country citizens: the *Cyber Awareness Calibration Instrument for Developing Countries* (Cyber4Dev-Q).

Section 2 reviews the related literature. Section 3 discusses the research methodology and Section 4 discusses the results. Questionnaire validation is addressed in Section 5. Lessons learned and future work are discussed in Section 6. Section 7 concludes.

2 Literature Review

Security awareness is defined by Wolf et al. (2011,p. 2) 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 needs to calibrate itself (Wang et al., 2018) (Figure *1*) i.e., to (1) measure baseline cyber awareness of a community before delivering training, and (2) measure the success of the awareness programme afterwards to refine subsequent awareness and training drives (Wolf et al., 2010). This calibration ensures that training remains relevant and effective by targeting revealed awareness deficiency areas (Gundu et al., 2019).

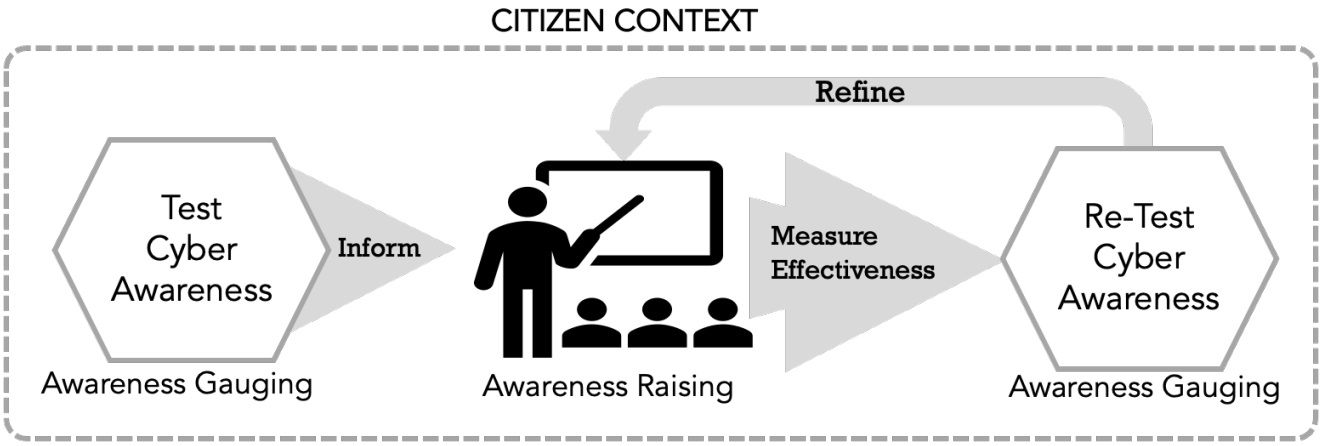

Figure 1: Cyber Awareness Raising Stages

Hence, it would be useful to have a questionnaire that specifically accommodates the needs of individual developing country citizens, as outlined in the following sections. Section 2.1 presents definitions of the three core cyber concepts. Section 2.2 then discusses the Cyber 4 Development research field. Section 2.3 discusses the South African context. Section 2.4 reviews other cyber awareness surveys that have been developed. Finally, Section 2.5 summarises the paper.

2.1 Cyber Concepts

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

Grey (2011, p. 77) defines **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). Cybersafety 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. Cybersafety education also involves guidance on cyberethics to form a responsible attitude to the use of ICT*". (References embedded in the definition by Grey)

Craigen, Diakun-Thibault and Purse (Craigen et al., 2014, p.16) define **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 (Westin, 1968, p.7) defines 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.

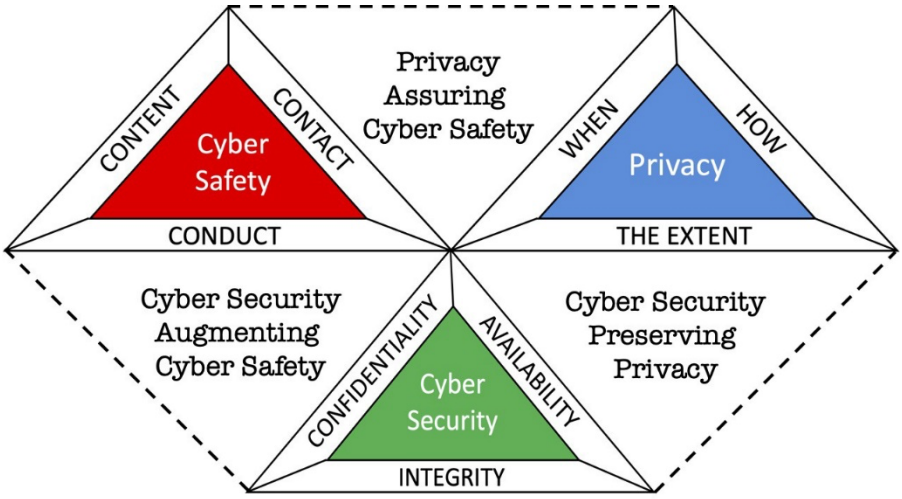

Figure 2: Dimensions of the three related cyber concepts.

Figure 2 depicts the dimensions of the three concepts, and their interdependencies. For example, the use of a VPN (Virtual Private Network), a security measure, can also 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.

For the rest of this paper, we shall use the term 'cyber' 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, 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 low cyber risk literacy and that various countries do not prioritise nor assess the country's cyber risk education needs. The index clearly illustrates that developed countries are at the top of the index, such as Switzerland, Singapore, United Kingdom, Australia and the Netherlands. Several of the 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 cybersecurity challenges. Public awareness of cybersecurity is low, with Internet users having neither the necessary awareness nor 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 cybersecurity systems with few operational Computer Emergency

Response Teams (CERTs) (Calandro and Berglund, 2019; van der Spuy, 2018). A policy brief of the United Nations (United Nations (UN), 2014) (NTIS/002/2014) states that Africa faces a number of Internet-related obstacles, with most governments on the continent lacking the technical or financial ability to target and monitor the majority of them. This is exacerbated by a lack of 'computer' skills with only half of African schools including this in the school curricula, as compared to 85% globally (Kandri, 2019).

A number of cyber-related interventions have taken place, including training sessions and workshops, often arranged or sponsored by developed countries. For example, the Council of Europe established the GLACY (and its extension, GLACY+) and ran cyber crime and policy workshops in Southern Africa (Global Action on Cybercrime, 2016). The ITU operated cybercrime workshops in 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). The EU-funded Cyber Resilience for Development (European Union Funded Project, 2017) 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 that was specifically tailored to the developing country context. This might have made calibration difficult.

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, 2021). South Africa 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 has been estimated to reach 26.3 million by 2023, giving even more people access to cyberspace (Statistics South Africa, 2020). Cyber awareness is 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 yet been formulated to achieve this (Sutherland, 2017).

South Africa faces a number of specific challenges (Key Differences, 2020; Leader, 2011; McDowell, 2010): (1) low per capita income, (2) poverty & unemployment, (3) inequality, (4) 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) low performance of public services. Many of these potentially impact citizen cyber awareness and relevant skill development as illustrated by the Cyber Risk Literacy and Education Index

showing that South Africa scored low across all categories including that of cyber risk awareness and educational inclusivity. (Oliver Wyman, 2021).

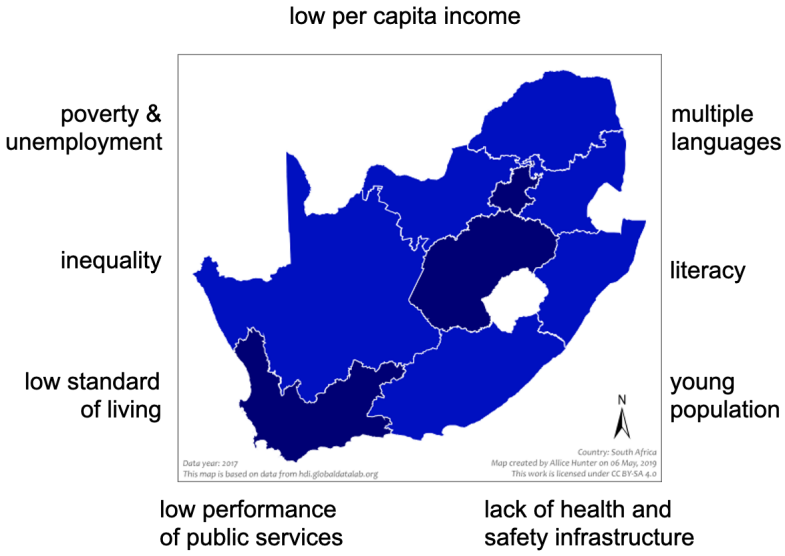

Figure 3: South Africa's Challenges (Map by Allice Hunter from: https://commons.wikimedia.org/wiki/File:South_African_provinces_by_HDI_(2017).svg)

South African academics are active in supporting cyber awareness raising efforts (Venter et al., 2019; Nagyfejeo and Von Solms, 2020; Aldawood and 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 due to the high unemployment levels (Trading Economics, 2021) with an especially low drive for cyber literacy and unequal access to technologies and education

The South African context is different from any developed country context. That being so, in designing Cyber4Dev-Q, we should acknowledge the impact of the developing context so as to ensure that the instrument measures cyber awareness as effectively as possible. In essence, while the 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 enhances 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) argue 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*". 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 1 provides the authors, followed by column two with 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" 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, but their intervention is not targeted towards individual citizens, but rather for a workplace context. Egelman et al. (2016) focused on the development and validation of the Security Behavior Intentions Scale (SeBIS). While this questionnaire covers a range of cyber security topics, it does not include cyber safety concepts. Parsons et al. (2017) developed the HAIS-Q questionnaire. This questionnaire's questions also relate to the workplace context and the questionnaire was validated with Australians i.e. developed country citizens. The HAIS-Q questionnaire has been used in various studies in an organisational context (Dharmawansa and Madhuwanthi 2020, Saridewi and 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 about Internet usage. Similarly Zulfia et al. (2019) also used HAIS-Q in an organisational study in Indonesia with recommendations focussing on organisational improvement of awareness about information security policies and technology. The Cyber Risk Literacy and Education Index (Wyman, 2020) highlighted the fact that in various geographical regions awareness and teaching of cyber risks is driven by organisations with governments lagging in this regard. This resonates with the academic research in cyber awareness 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 instrument focussing on the general user or individual (Velki & Šolić, 2019, Egelman et al. 2016), the questionnaires are 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 a *culture* of security (Hayden, 2015; Schlienger and 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 for 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 Instruments (•=satisfies; Ø=fails)

Reference	Description	Comprehensiveness	Individual Focused (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)	Behavioral-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 questionnaire for employers	Cyber Safety Cyber Security	Ø	Ø	Australia
Wahyudiwan et al., 2017	KAB (Knowledge, Attitude, and Behavior model) for organisations	Cyber Safety and Cyber Privacy excluded	Ø	Ø	Indonesia
Balhara et al, 2018	Generalized Problematic Internet Use Scale 2	Cyber Safety Only		Ø	India
Nilsen, 2017	MyCyberKSAsTM prototype tool, organisational awareness	Cyber Security Only	Ø	Ø	USA
Akhter et al., 2020	Problematic Internet Use (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,	Cyber Security Only	•	•	Israel, Slovenia, Poland and Turkey

Reference	Description	Comprehensiveness	Individual Focused (not workplace)	Country Context-Sensitive	Country
	knowledge and behaviour				
Elradi et al., 2020	Cyber security awareness	Cyber Security Only	●	●	Sudan
Evans et al. (2019)	IS-CHEC information security Human Reliability Analysis (HRA) technique	Cyber Security Only	Ø	Ø	United Kingdom
Grassegger & Nedbal, 2021	Security awareness program for organisations	Cyber Security Only	Ø	●	Austria
Alzubaidi, 2021	Measuring security awareness for cybercrime	Cyber Security Only	●	●	Saudi Arabia

2.5 Summary of Requirements for the Questionnaire

In summary, when cyber awareness drives are carried out, it is essential to ensure that they have achieved their aims. In other words, there is a need to assess awareness both before and after awareness drives. This ensures that the training is targeted, relevant and topical, and accommodates the developing country context. This confirms the need for a questionnaire that meets the following requirements:

(1) **Comprehensive**: incorporating constructs to measure awareness of all three cyber concepts. (Given that the concepts, and required precautions, are substantively different - Section 2.1).

(2) **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 languages) are not necessarily prioritised (accommodating the context and challenges of the under-served, under-resourced, and under-represented – Section 2.2).

(3) **Individual-Focused**: being aimed at individuals, as opposed to employees or organisations, as discussed in Section 2.3.

3 Developing Cyber4Dev-Q

This research study was conducted in South Africa and hence the South African context, as a developing country, had to be considered for the development of the questionnaire. To ground our questionnaire in the

developing country context, we consulted the Cyber Security Awareness Workbook published by the South African Cyber Security Academic Alliance (SACSAA) (SACSAA, 2020) 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. 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.

Of the topics in the workbook, online etiquette 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, 2012) (developed in South Africa) was also consulted. This Guide's aim was to raise awareness of the potential cyber risks that South Africans face. They also provide guidelines to inform end users. We also consulted other awareness-raising questionnaires to ensure that all pertinent cyber-related aspects were covered (Parsons et al., 2014; Egelman et al., 2016). We also consulted South African government statistics and news reports reporting on cyber-related crimes and issues in South Africa.

Table *4* in the Appendix consolidates our findings, the themes and theory for the items included in our questionnaire. Citations refer to the source of each individual question. The questionnaire statements were phrased from an individual, as opposed to an employee, perspective. For example, when advising reporting, the advice was that they should direct these to a local authority or cyber group in the community who are able to support them on an individual level, instead of their organisation's IT department.

3.1 Survey Method

A positivist paradigm was followed to establish measurable facts about the cyber awareness in a community using a quantitative approach (Saunders et al., 2009) being effective when the intention is to describe the attitudes or opinions of a population (Creswell and 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 and 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). 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. The Statistical Package for the Social Sciences (SPSS) was used to perform descriptive and inferential statistical analysis.

3.2 Instrument Development

The Cyber4Dev-Q comprises of three sections:

(1) *content questions* to understand the context such as what devices respondents use and for what purpose, where they currently obtain information about cybersecurity and their preferred communication methods,

(2) *cyber awareness* questions adapted from the SACSAA themes and categorized according to cyber safety, cyber security and cyber privacy as well as questions tailored to the developing country challenges. The SACSAA themes were used to develop each of the questions in the Cyber4Dev-Q as depicted in Table 4 in Appendix A.

(3) *demographic questions*.

An introduction letter, information document and consent form were included, explaining the objectives of the research, explaining that responses would be anonymous, and 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, seventeen participants completed a hard copy of the questionnaire and provided feedback in terms of how easy the questions were to understand, and questionnaire length. Only minor changes were made, and the background questions refined based on their feedback. The questions, and their application to the different cyber concepts, are depicted in Figure *4*.

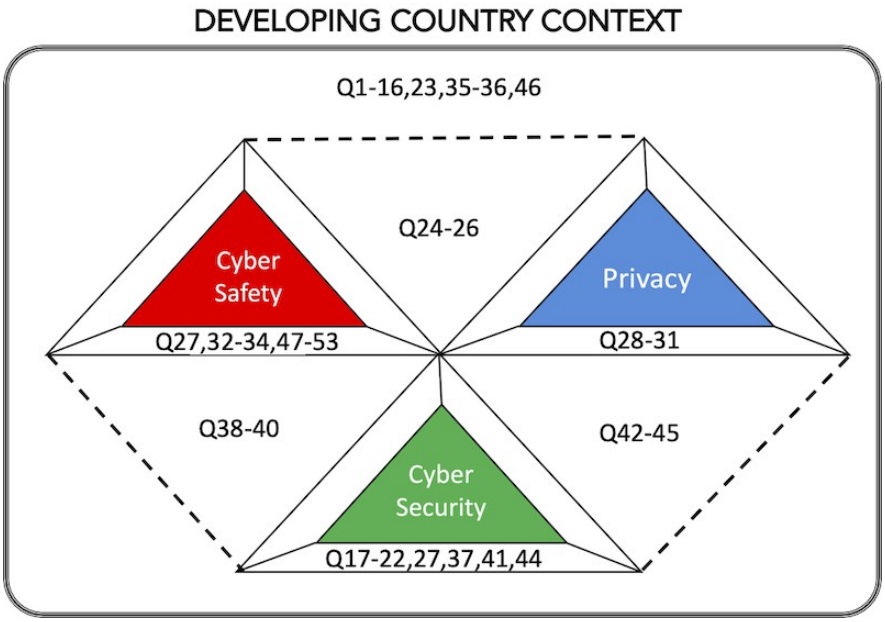

Figure 4: Allocation of Questions to Cyber Concepts and Co-Dependencies

3.3 Sample and Data Collection

Data was collected during the Chance2Advance event [Anonymised for Review]. This annual event takes place in so as to communicate with, educate and enrich participants through a variety of workshops. It took place at the Ebenezer AME church in [City]. [City] 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, and as a result, [City] is deemed to be an urban area. Due to the legacy of apartheid [City], 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 half of the community has access to the Internet (Census 2011, 2011).

[City] residents who attended the community workshop session hosted by the university were asked to complete the survey. A total of 160 people attended this cyber workshop, of whom 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).

For a demographic profile of the respondents, see **Table 2**. 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 [Anon] 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

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

4 Results

The data gathered in the [Anon] community indicated that the profile of the community was mostly generation Y, with only a school qualification, all of whom owned either a mobile phone, laptop or tablet.

4.1 Content question results

The questions in the content section of the questionnaire indicated that all respondents used a mobile phone – mostly for phone calls (95%), for instant messages (such as SMS or WhatsApp (82%)), to browse the Internet (77%) and to access social media sites (e.g., Facebook or Twitter (73%)). A number of them used their mobile phones to send emails, play games or watch videos, and 47% used their phones for Internet banking. Not all respondents had access to a home computer (53%) or tablet (44%), but those who did, used these for a variety of online activities. The word clouds (see Figure *5*) reflect the activities, which respondents indicated under the "other" option for the use of their mobile phone, tablet and home computer, respectively. Work is a common theme, while listening to music is a key activity.

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% indicated 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%).

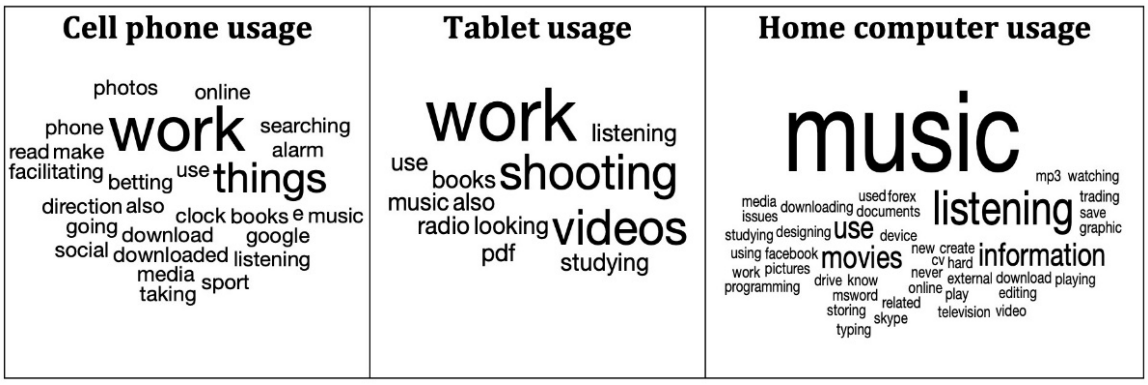

Figure 5: Usage of devices

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

4.2 Cybersecurity awareness question results

A summary of the key results of questions 17–53 is presented below in the three themes, namely cyber safety, cyber security and cyber privacy.

Developing Country Context:

Reporting: Only 32% of community members knew how and where to report a cyber related incident or crime. 68% said that they had never fallen victim to this type of crime. This could be due to their not knowing that they had experienced an attack.

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%).

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 indicated that they used a password on all their devices (83%), and made use of upper case, lower case, special characters and numbers (69%). They also knew about anti-virus software (61%), but only 48% had installed this 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 developing country citizens.

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

Cyber Privacy: Some 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 a policy, only 50% knew how to change their default privacy settings, and 59% indicated that they understood such policies. The respondents believed they were safe in cyberspace and could do anything they wanted to, as

long as they stayed 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 IP address unless they are using a 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 SPSS, was conducted on Cyber4Dev-Q, questions 17–53. The data were subjected to Bartlett's Test for Sphericity and the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy, to test the aptness of the sample for the EFA (Kaiser and Rice, 1974). Bartlett's Test for Sphericity 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 (Kaiser and Rice, 1974), the KMO should be 0.60 or higher in order to proceed with factor analysis. Six factors were identified (**Table *3***), with a KMO value of 0.670. Kaiser recommends 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 six factors could be extracted (Kaiser and Rice, 1974).

Only items with a value above 0.4 were retained, having been deemed meaningful (Gerber and Hall, 2017) (Q23, Q33, Q35 and Q53 were thus removed). The Cronbach alpha values were all above 0.6, which is deemed acceptable (Gerber and 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 alpha for each factor.

Table 3: New factors and Cronbach alpha values (developing context questions in bold)

Factors	New Factor Names	Item Numbers	Total Items	Cronbach 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

5.2 Cyber4Dev-Q questionnaire improvements

To improve the Cyber4Dev-Q questionnaire, based on the outcome of the EFA in SPSS, more items can be added to factors 4 and 6, to have at least three items per factor (O'Rourke and 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 emails 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 in Appendix A next to the applicable statements. The six new factors are listed below with a short description of the purpose of each factor based on the questions that are grouped per factor as per the EFA.

F1: *Cyber safety and privacy risk awareness*: Perception about the risk and threats in cyberspace pertaining to safety and privacy

F2: *Cyber security protection*: Technical controls for protection in cyberspace

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

F4: *Cyber safety risks*: The personal experience of cyber risks

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

F6: *Cybersecurity for passwords*: Focusing on the secure password practices in cyberspace

6 Discussion

It clearly cannot be assumed that rural and urban South African citizens will 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). This 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 obviously not common knowledge to all computer users, especially those living in developing countries.

Our investigation confirmed that developing country citizens require a context-sensitive approach to address the risk they face from cyberspace. The results of this study confirmed the need for targeted awareness and training presentations, or workshops delivered by experts in South Africa. It also confirmed the special challenges faced by these citizens that confirm the need for a questionnaire which specifically acknowledges their challenges and is designed to accommodate them.

We now return to the requirements of the questionnaire, to reconsider whether Cyber4Dev-Q satisfies them:

(1) **Comprehensive**: the questionnaire incorporates constructs to measure awareness of all three cyber concepts: cybersafety, cybersecurity and privacy (Figure *4* and **Table *5***).

(2) **Country Context-Sensitive**: we have included context-specific questions based on the South African context, and our validation process revealed the importance of these questions in understanding the challenges of cyber awareness (Figure 5).

(2) **Individual-Focused**: we did not include questions which could be specific to the organizational context, in particular related to reporting of incidents.

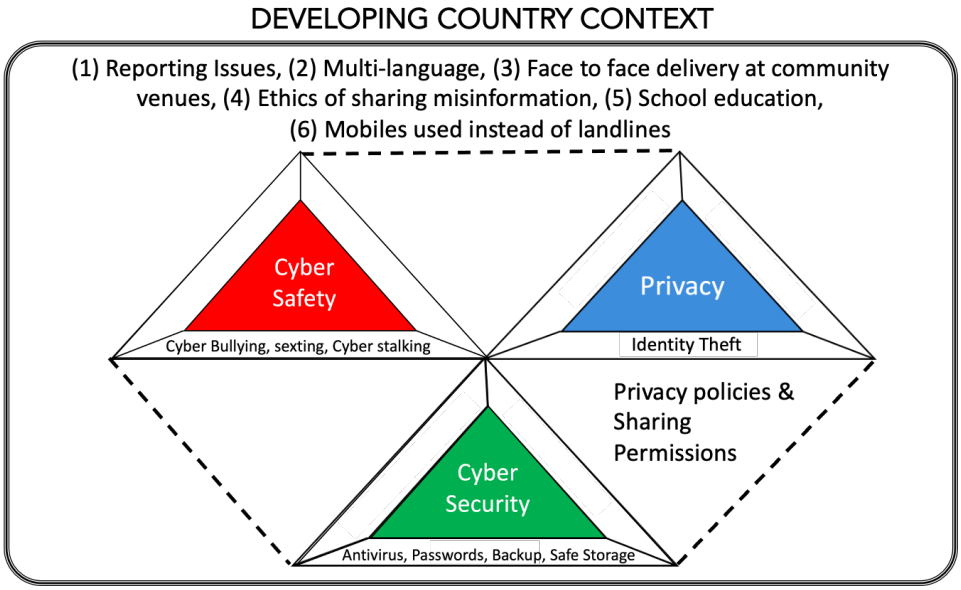

Figure 6: Refinements of Security Training

6.1 Practical Implications

Using the Cyber4Dev-Q revealed the following areas where future cyber awareness raising efforts should focus:

Developing Country Context:

- **Reporting**: They need to know where and how to report cyber related crimes and incidents, which channels exist for this purpose in South Africa. (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 should be sensitive to this reality. As Sotho was the first language of most respondents, future workshops should be delivered in Sotho. Security

awareness drives should also be sensitive to the demographic profile of the community. (Multiple Languages).

- **Delivery Method**: Electronic communications can be utilised and distributed via existing community structures (e.g., churches or schools using e-mails, sign-up to monthly awareness-raising e-mails or social media such as Facebook). Workshops, including face-to-face presentations, are preferred and are thus the optimal deliver mechanism in this developing country context. (Low literacy levels).
- **Ethics**: Regarding the sharing of inaccurate or incorrect information in cyberspace. (Different laws).
- **Device**: The awareness raising programme should focus on mobile phones, as opposed to laptops and iPads, as the majority of South Africans use a mobile phone to access cyber space. (Literacy and education, inequality and poverty).

Cyber Safety:

They need to be informed on how to deal with cyber bullying, stalking, identity theft and unwanted sexting. This is of importance from a young age to include education in primary and secondary school education and curriculums. These topics can be incorporated in the proposals of the Department of Basic Education of the country when designing the planned digital stills strategy for South Africa (BusinessTech 2020).

Cyber Security:

The use of antivirus programs: where to download them and how to use them; physical security of devices and how to make backups. Finally, the password “best practice” possessed by these citizens is now outdated. Latest “best practice” guidelines suggest that length, not complexity, ought to be maximised (Grassi et al., 2017; Centre for the Protection of National Infrastructure, 2015; UK Government, und). Cyber4Dev-Q should be updated to reflect these, as should the training itself.

Cyber Privacy:

Where to find website privacy and security policies, what the policies typically cover and mean, how to change the privacy settings of their social media accounts. Privacy terms and conditions of mobile applications should also be addressed. This is particularly important as the data protection act, Protection of Personal Information Act of 2013 (Department of Justice, 2013), of South Africa came into force on 1 July 2020 with the grace period elapsing on 1 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 the native languages must be included in campaigns and not only English, 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 our hope that independent organisations can leverage the data gathered via the Cyber4Dev-Q to inform the content of their outreach programmes to focus on the revealed areas of cyber safety, security and privacy that required more focused attention, see Figure *6*.

6.2 Research Implications

Our study highlights the importance of context in measuring cyber awareness. The context we focused on was the developing country context. We realised that there was no existing instrument tailored towards the measurement of cyber awareness in this context, which is why we developed Cyber4Dev-Q. Other researchers have developed questionnaires for country-specific studies, but these have generally only been used for the single study and in an employee-organisational context. With respect to future research, it is important for further research to be carried out in the following areas:

(1) Develop ways to feed a particular country's context-specific needs into 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 which they mine to match their particular country context.
(2) Develop 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. We need to design revisions into our survey instruments or risk them becoming outdated and teaching sub-optimal principle.
(3) Some computer users are particularly vulnerable in this space. These might be senior citizens, those with cognitive disabilities or those who do not understand English very well. We should also find a way to meet their needs in this space (Renaud, 2021).

7 Limitations

A limitation of the study is that the Cyber4Dev-Q was validated in a single community in South Africa. As future research, Cyber4Dev-Q will be administered to other community groups across South Africa and in other African countries to develop more questions that can be used in a question bank. Cyber4Dev-Q will be refined and improved using factor and item analysis of this study.

Actual behaviours are not measured by any survey instrument and Cyber4Dev-Q does not offer the opportunity to confirm the veracity of responses. That being so, we plan to conduct interviews with developing

country citizens, in their home language. This will enable us to obtain richer data to inform cyber awareness and training programmes based on the outcome of Cyber4Dev-Q in the local area.

8 Conclusion

The objective of this study was to develop a cyber awareness measurement instrument that satisfied three requirements (Cyber4Dev-Q): (1) country context-sensitive: designed for the developing country context (the under- served, under-resourced, and under-represented), (2) comprehensive: including questions about all three cyber concepts, and (3) individual-focused, as opposed to targeting employees within organisations. Cyber4Dev-Q was validated in an urban city in South Africa, and revealed clear cyber awareness gaps, which can now inform future cyber awareness drives. Cyber4Dev-Q is the first context-sensitive cyber awareness measurement instrument which accommodates the needs of developing country citizens. We hope that researchers will test this instrument in other developing countries. Our aim 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 Questionnaire is available for download from [Anonymised for Review].

References

Alzubaidi, A., 2021. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1), e06016.

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.

Aldawood, H. and Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In *IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68. IEEE.

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575.

Arde, A. (2014). Cellphone cover: the smart thing to do. Retrieved 30 June 2021 from: https://www.iol.co.za/personal-finance/cellphone-cover-the-smart-thing-to-do-1759957

Bada, M., Von Solms, B. and Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in Africa: An empirical study. In *3rd International Conference on Cyber-Technologies and Cyber-Systems*, 78–83.

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.

Banciu, D., Rădoi M. and Belloiu, S. (2020). Information security awareness in Romanian public administration: An exploratory case study. *Stud Informatics Control*, 29, 121–9.

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. Paper presented at the *Early Childhood Convention*, Rotorua, New Zealand.

Benson, V., Saridakis, G. and Tennakoon, H. (2015). Information disclosure of social media users. *Information Technology & People*, 28(3), 426–441.

Blue Turtle Technologies (2020). Cyber Crime a pandemic hitting the wallet of South African business.https://www.itweb.co.za/content/JN1gPvOYBWPMjL6m.

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

BusinessTech (2020). These are the skills government wans 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/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf.

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

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.

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.

Creswell, J. W. and Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Dharmawansa, A.D. and Madhuwanthi, R.A.M. (2020). 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, 147-154, KDUIRC.

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.

Department of Justice (2013). Protection of Personal Information Act 4 of 2013. Government Gazette, pp. 1–76. Cape Town, Republic of South Africa.

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 2016 CHI conference on Human Factors in Computing Systems,* 5257–5261.

Elgot, J. (2015). One in five young people has suffered online abuse, study finds. Retrieved 10 April 2021 from: 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.

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H. and 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(2019), 102087–102101.

European Union Funded Project (2017). Cyber 4 Dev. Retrieved 23 February, 2021 from https://cyber4dev.eu/.

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.

Funke, D. and Flamini, D. (2018). A guide to anti-misinformation actions around the world. https://www.poynter.org/ifcn/anti-misinformation-actions/.

Gerber, H. and Hall, R. (2017). Quantitative research design. HR Statistics Pty, South Africa.

Ginosar, A. and Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? *Information & Management*, 54(7), 948–957.
Global Action on Cybercrime (2016). Strategic priorities for cooperation on cybercrime and electronic evidence in GLACY countries. https://www.coe.int/en/web/cybercrime/ glacyplus-launching-conf.
Global Forum on Cyber Expertise (2019). Cybercrime Model Laws Discussion paper prepared for the Cybercrime Convention Committee. 1-5 September. https://cybilportal.org/.
GOV.UK (2020). Cyber Security Breaches Survey 2020. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber- security-breaches-survey-2020.
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.
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. Technical report, NIST. https://pages.nist.gov/800-63-3/sp800-63b.html Accessed September 2019.
Grey, A. (2011). Cybersafety in early childhood education. *Australasian Journal of Early Childhood*, 36(2), 77–81.
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.
Grobler, M., Jansen Van Vuuren, J. and Leenen, L. (2012). Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. In ICT Critical Infrastructures and Society. HCC 2012. *IFIP Advances in Information and Communication Technology*, volume 386, 215–225, Berlin, Heidelberg.
Gundu, T., Flowerday, S. and Renaud, K. (2019). Deliver security awareness training, then repeat:{Deliver; Measure Efficacy}. In *2019 Conference on Information Communications Technology and Society (ICTAS)*, 1–6. IEEE.
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.
Hagen J.M., Albrechtsen E. and Hovden J. (2008) Implementation and effectiveness of organizational information security measures. *Information Management and Computer Security*, 16, 377–97.
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.
ITU (2014). LDCs Infrastructure Protection Program: Comoros. 1-5 September. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/LDC_Comoros.aspx.
ITU (2021). National Cybersecurity Strategies Repository. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx
Jamil, Z. (2014). Cybercrime model laws. https://rm.coe.int/1680303ee1.
Kahla, C. (2020). SA, Kenya and Nigeria report highest cyber attacks in Africa. 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.
Kandri, S.E. (2019). Africa's future is bright—and digital. https://blogs. worldbank.org/digital-development/africas-future-bright-and-digital.
Key Differences (2020). Difference between developed countries and developing countries. https://keydifferences.com/difference-between-developed-countries-and- developing-countries.html.
Kortjan, N. and von Solms, R. (2012). Cyber security education in developing countries: A South African perspective. *In International Conference on e-Infrastructure and e-Services for Developing Countries,* 289–297. Springer.
Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, 29(2), 16–35.

Kritzinger, E., Bada, M. and Nurse, J. R. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education*, 110–120. Springer.

Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4):289–296.

Lamp, J.W. (2017). Preface to Selected Papers from ACIS 2016. *Australasian Journal of Information Systems*, *21*.

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

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

Livingstone, S., Stoilova, M. and Nandagiri, R. (2019). Talking to children about data and privacy on- line: research methodology. http://eprints.lse.ac.uk/101284/1/ Livingstone_talking_to_children_about_data_published.pdf.

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

McDowell, M. (2010). Language Challenges in South Africa. 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.

Naik, S. (2021). SA youngsters under threat from cyber bullies as online shaming and revenge porn also on the rise. 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.

Nhlapo, Z. (2017). Sexting – The Shocking Pandemic Among South African Teens. 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. Retrieved from NSUWorks, College of Engineering and Computing.

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

Oliver Wyman (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 modeling. SAS Institute.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, 66:40–51.

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.

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. *Centre for Justice and Crime Prevention*, 13(6):1–16.

Renaud, K.,(2021). Accessible Cyber Security: The Next Frontier?. In *ICISSP* (pp. 9-18).

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.

SACSAA (2020). South African Cyber Security Academic Alliance (SACSAA), Cyber Security Awareness Workbook. Retrieved 30 September, 2019 from http://eagle.unisa.ac.za/elmarie/images/Pdf/book. pdf.
Saunders, M., Lewis, P. and Thornhill, A. (2009). Research methods for business students. Pearson Education, Harlow, UK.
Schlienger, T. and Teufel, S. (2005). Tool supported management of information security culture. In IFIP International Information Security Conference, 65–77. Springer.
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). Identity fraud and theft on the rise in South Africa compared to 2018. 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, Criminology, University of South Africa.
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 (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.
Sutherland, E. (2017). Governance of cybersecurity - The case of South Africa. *The African Journal of Information and Communication*, 20:83–112.
Trading Economics (2021). South Africa Unemployment Rate. https://tradingeconomics.com/south-africa/unemployment-rate.
Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008a). Investigating information security awareness: research and practice gaps. *Information Systems Security*, 17(5), 207-227.
Öłütçü, G., Testik, Ö.M. and Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 6:83–93.
UK Government (und). Ask users for passwords. https://design-system.service.gov.uk/patterns/passwords/.
Unwin, P. and Unwin, T. (2009). ICT4D: Information and communication technology 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 Electronic Computer Engineering Systems*, 10, 19–24.
Velki. T., Solic, K. and Ocevcic, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing work. International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 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. 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.
Westin, A.F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166–170.
Wilby, M. (2010). The simplicity of mutual knowledge. *Philosophical Explorations*, 13(2), 83–100.
Wild, S. (2020). Citing Virus Misinformation, South Africa Tests Speech Limits. https://undark.org/2020/04/03/fake-news-south-africa-covid-19/.

Wolf, M.J., 2010. Measuring an information security awareness program. University of Nebraska at Omaha.
Wolfpack Information Risk (2012). Cybercrime survival guide. www. wolfpackrisk.com.
Zulfia, A., Adawiyah, R., Hidayanto, A. N. and Budi, N.F A. (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.
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.

Appendix A

Table 4: Cyber Awareness Questionnaire (Cyber4Dev-Q) – initial 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 default privacy settings (Parsons et al., 2017; Wolfpack Information Risk, 2012)			•
Literacy and educational	Awareness of website privacy policy (Ginosar and Ariel, 2017; Benson et al., 2015)			•
Literacy	Reading of website privacy policies (Ginosar and Ariel, 2017; Benson et al., 2015)			•
Literacy and educational	Understanding of website privacy policies (Ginosar and 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 possibility of cyber bullying (SACSAA, 2020; Naik, 2021; Elgot, 2015; Popovac and Leoschut, 2012)		•	
	Perceptions about cases of cyber bullying (SACSAA, 2020; Naik, 2021; Elgot, 2015; Popovac and Leoschut, 2012)		•	
Educational	Experience of sexting (Kritzinger, 2017; Nhlapo, 2017)		•	
	Perceptions about friends experiencing sexting (Kritzinger, 2017; Nhlapo, 2017)		•	
CYBER SECURITY				
Infrastruct-ure	Backing up information (Egelman et al., 2016; SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Literacy and educational	Knowing what antivirus is (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Basic Principles	Having antivirus 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)	•		

Context		Cyber Topic		
Section 2.3 Challenge	**Item to include in questionnaire**	**Sec**	**Saf**	**Priv**
Literacy	Using a password on devices (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		
Literacy	Using strong passwords (Parsons et al., 2017; SACSAA, 2020; Wolfpack	•		
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 backups (SACSAA, 2020)	•		
Literacy and low per	Perceptions about banking credentials being stolen in Cyberspace (SACSAA, 2020)	•		
	Perceptions about phishing (responding to unknown emails) (SACSAA, 2020; Wolfpack Information Risk, 2012; Walker, 2020)	•		
	Perceptions that device can become infected (SACSAA, 2020; Wolfpack Information Risk, 2012; Kahla, 2020)	•		
	Perceptions that device can be implicated in a crime (Wolfpack Information Risk, 2012; Africa Check, 2020)	•		
	Perceptions that criminals can access device (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 cyberspace (SACSAA, 2020; Wolfpack Information Risk, 2012)	•		•
CYBER SAFETY & CYBER SECURITY				
Public service	Awareness of reporting cyber incidents (SACSAA, 2020; Wolfpack Information Risk, 2012)	•	•	
Public service	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	Perceptions about posting inaccurate information (SACSAA, 2020; Wild, 2020; Funke and Flamini, 2018)	•	•	

Table 5: Cyber Awareness Questionnaire (Cyber4Dev-Q) – results of analysis

Statements	New Factors
17. I know what an anti-virus software program is.	F2
18. I have an anti-virus software program installed on the computer that I use.	F2
19. I know what a personal firewall program is.	F2
20. I have a personal firewall program installed on the computer that I	F2
21. I use a password on all my devices.	F6
22. My passwords consist of upper case, lower case, special characters	F6
23. 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
24. I do not give out my personal information (like real name, age, location, etc.) when using online gaming applications.	F5
25. I do not post information (e.g. messages or photos) about my friends	F5
26. I do not respond to unwanted communications or messages from people I do not know (like emails, WhatsApp, Facebook messages, etc.)	F5
27. 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
28. I changed the default privacy settings of my social media accounts.	
29. I know where to find a website's policy which explains how the website will protect my information.	
30. I read website policies relating to how my information is protected (e.g. privacy policy, security policy or terms and conditions) on websites	F3
31. I understand website policies relating to how my information is protected (e.g. privacy policy, security policy or terms and conditions) on websites.	F3
32. I have NEVER been victimized in cyberspace (e.g. via social media like Facebook, Twitter or WhatsApp).	F3
33. I feel comfortable telling someone if something made me feel uncomfortable while using cyberspace (e.g. Facebook twitter, WhatsApp, SMS etc.).	Removed, <0.4 Move to Yes/No
34. I only add friends to my social networking profile if I know them.	F3
35. I know where to report a cyber security incident or crime.	Removed, <0.4, Move to Yes/No
36. No one that I know has ever experienced difficulty in reporting when they are victimized/harassed/bullied via a mobile phone or social media.	F3
37. 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
38. I believe that it is possible that my device can be implicated in cybercrime (this means, it looks as though the crime was committed using my device).	F1
39. I believe that criminals can access one's device (e.g. laptop, tablet) through cyberspace and the information on it without physically having access to my device.	F1
40. I believe that if a device is lost or stolen the information could be used for criminal purposes.	F1
41. I believe it is important to back up information that is on my devices.	F1
42. I believe it is possible that one's identity can be stolen in cyberspace.	F1

Statements	New Factors
43. I believe it is possible that one's personal information can be stolen in cyberspace, e.g. while playing online games or when using some apps.	F1
44. I believe that it is possible that one's bank accounts could be compromised and money stolen in cyberspace.	F1
45. 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
46. I (or my friends) believe it is unacceptable to post or share inaccurate or incorrect information in cyberspace.	F1
47. I am aware that I can be stalked (e.g. online predators, harassment, unwanted communication) in cyberspace.	F1
48. I believe my friends are aware that they can be stalked (e.g. online predators, harassment, unwanted communication) via an electronic device.	F1
49. I believe that I can be bullied in cyberspace (e.g. via social media).	F1
50. I believe some of my friends have experienced cyber bullying (via an electronic device).	F1
51. I have experienced unwanted sexting in cyberspace (e.g. via WhatsApp or Facebook).	F4
52. I believe some of my friends have experienced unwanted sexting in cyberspace (e.g. via WhatsApp or Facebook).	F4
53. I believe I am safe in cyberspace when doing anything that I want, as long as I stay anonymous or use a fake name.	Removed, <0.4, Move to Yes/No