information

MDPI

Article

Improving Cybersafety Maturity of South African Schools

Elmarie Kritzinger

Department of Information System, School of Computing, College of Science, Engineering and Technology, Florida campus, University of South Africa, Corner of Christiaan de Wet Road & Pioneer Avenue, Florida 1709, South Africa; kritze@unisa.ac.za

Received: 1 August 2020; Accepted: 2 September 2020; Published: 4 October 2020

Abstract: This research investigated the current maturity levels of cybersafety in South African schools. The maturity level indicates if schools are prepared to assist relevant role players (teachers and learners) in establishing a cybersafety culture within the school environment. The research study measured the maturity levels of cybersafety in 24 South African schools by evaluating the four main elements that are needed to improve cybersafety within schools. These elements are (1) leadership and policies, (2) infrastructure, (3) education, and (4) standards and inspection. The study used a UK-approved measurement tool (360safe) to measure the cybersafety maturity of schools within South Africa, using five levels of compliance (Level 1: full compliance, to Level 5: no compliance). The data analysis clearly indicated that all the schools that participated in the study had a significantly low level of cybersafety maturity and compliance. Schools are starting to adopt technology as part of their educational and social approach to prepare learners for the future, but there is a clear lack of supporting cybersafety awareness, policies, practices and procedures within South African schools. The research proposed a step-by-step approach involving a ten-phase cybersafety plan to empower schools to create and grow their own cybersafety culture.

Keywords: cybersafety; awareness; school learners; knowledge and skills; culture; maturity

1. Introduction

A global trend that is growing exponentially is connectivity to the internet (in other words, cyberspace entry). Cyberspace is defined as an environment in which users communicate and connect via a network with other users across the globe. Users who use the internet to connect to cyberspace are called cyber users. Cyber users range in age, gender, nationality and geographic location, among other characteristics. Connectivity to cyberspace is changing the social dynamics of environments through cyber actions by individuals, public social groups and institutions [1]. According to Randa [2], "the cyber-social environment has added a dimension to social context that has had an undeniable cultural impact in a relatively short period of time". Social dynamics within cyberspace are different from those in the real world, and the social interactions (public and/or private) within cyberspace are changing cyber users' actions, activities and participation with other cyber users. These social interactions with other cyber users include activities such as communication and knowledge gathering, and those include education- and financial-related activities [3]. When cyber users connect to cyberspace, they are dependent on the rules of cyberspace, or more accurately, the lack thereof [4]. When users access global networks, they are confronted by the unique challenges of cyberspace.

Currently, cyberspace is shared by almost half of the world's population—it has 3.5 billion users [5]—and has grown to be the most-used technology worldwide. It has invaded all societies and has a wide impact, ranging from financial implications to social interactions [6]. Cyberspace

has changed the social dynamics of environments, cultures and even belief systems. It is, therefore, vital that research is conducted to investigate the impact of cyberspace on society to ensure that all individuals within a specific society have the required knowledge and skills to become a cyber citizen, and to be safe within cyberspace. A group of cyber users that is extremely vulnerable to cyberthreats and victimisation is school learners [7,8]. Unfortunately, few studies have been done to fully understand the impact of cyber-related issues on school learners [9,10]. School environments are "living ecosystems" and are in a unique space to act as external role players that can assist and provide learners with the necessary cybersafety awareness, knowledge and skills to protect themselves in cyberspace.

Currently, however, schools are not contributing to establishing and growing a cybersafety culture among school learners, leaving learners vulnerable and open to cyber risks and threats. It is critical that any country or educational sector validate whether schools are becoming involved in cybersafety awareness and education [11,12].

There are different viewpoints on cybersafety and cybersecurity, and different definitions linked to these terminologies. Cybersecurity can be defined as the level of securing information within an organisational environment [13]. Cybersecurity focuses more on the technical aspects to protect information in cyberspace, for example best practices, safeguards and risk management assurance [14]. Cybersafety on the other hand focuses more on non-technical/ human-related aspects of protecting information within cyberspace. Cybersafety also focuses more on social interaction, ethics and behaviour among users within cyberspace [15]. Cybersafety awareness is meant to ensure that cyber users have the needed awareness regarding all aspects related to cyber risks and threats in order to protect themselves and their information within cyberspace.

This research focused primarily on the maturity of South African schools by measuring different aspects of cybersafety readiness, and made an overall contribution to establishing a cybersafety society within the schools. Cybersafety maturity is defined in this research as the readiness of schools to include cybersafety within the school environment. The research focuses on understanding what is currently being done in schools and where schools are lacking in providing a safe cyber environment for school learners in South Africa. The main research questions for this research include (1) Do South African schools have the maturity to assist school learners regarding cybersafety awareness?, and (2) How can South African schools be assisted to improve their cybersafety maturity if needed? The research objectives for this research include (1) an investigation to measure the maturity of South African schools and (2) identifying different countermeasures that can be implemented within the school environment to improve cybersafety maturity in schools.

The scope of the outcomes (linked to the research objectives) of this research includes (1) the analysed viewpoint of the current cybersafety maturity of South African schools, and (2) proposed guidelines that schools can implement to create and/or improve the cybersafety culture within South African schools. The contribution of the research is to plot the cybersafety maturing of schools within South Africa. The contribution also includes a proposed guideline that can assist schools to improve their cybersafety maturity within schools.

The article is divided into the following sections: Section 1 (this section) provides an overview and introduction to the research. Section 2 aims to provide a literature review regarding the main focus of the research, which includes cybersafety for schools. Section 3 provides the methodology of the research. Section 4 focuses on data gathering, data analysis and discussions on the research findings. Section 5 proposes cybersafety guidelines that can assist schools to improve cybersafety within the school environment. Section 6 concludes the research and provides insight into future research that can be conducted in this research field.

2. Cybersafety for Schools

Cyberspace has numerous advantages that include work-related activities, socialisation, entertainment, education and information gathering. An area where cyberspace is becoming more

prominent is the education environment. Preparing school learners for the 4th Industrial Revolution and equipping them with 21st century learning skills have become a global mandate within the education environment. More school learners have access to Information Community Technology (ICT) and ICT devices (mobile phones and tablets), and cyberspace. According to Kritzinger [16], more than 90% of school learners in South Africa have mobile phones, with the majority of the phones having internet connectivity. This allows school learners to access cyberspace, in many cases without the involvement (monitoring) of parents [17,18]. Terminology related to cyberspace includes cybersecurity and cybersafety that is linked to protecting users within cyberspace. There are a number of different viewpoints related to defining cybersecurity and cybersafety.

The advantages of access to cyberspace come with a downside that includes cybercrimes (risks and threats) that can cause harm to the cyber user, especially school learners [19]. It is important to note that cyberspace does not differentiate between adults and children. Age is irrelevant, and all users are equally susceptible to cybercrime. These cyber risks and threats include cyberbullying, sexting and violation of privacy [20]. Learners are using ICT and ICT devices increasingly within their learning environment (at school), and it is becoming more important to educate them on cybersafety [3,21,22]. Schools have a mandate to protect learners and ensure their safety within the educational learning environment [23,24]. Globally, school learners are seen as an easy target for cyber criminals to prey upon and exploit [25,26]. Schools play a vital role in cultivating and growing a cybersafety culture within the school environment [12,15,27]. The questions that arise include the following: Are schools prepared or properly equipped by government and management authorities to engage in cybersafety awareness? Are schools (within South Africa) contributing to growing a cybersafety culture among school learners? How do schools assist schools, teachers and school learners? All these questions contribute to the rising concern that not enough is being done to support school learners in their social and educational activities within cyberspace. This research investigated the maturity of South African schools and their readiness to ensure cybersafety, and considered how to change the current culture for the safety of schools, teachers and learners. The investigation focused on four main factors that address cybersafety readiness, namely leadership and policies, infrastructure, education, and standards and inspection.

Educators (teachers) play a vital role in the cybersafety education process within the school environment and among school learners [28,29]. However, cybersafety should ideally be addressed by school management, not by the teachers and learners. Teachers within South African schools are ill-equipped to deal with issues related to cybersafety due to a lack of knowledge and skills [16,28,30]. This research focused primarily on the improvement of cybersafety within South African schools in order to align with international cybersafety initiatives for teachers. However, before the cybersafety of teachers can be addressed, the cybersafety maturity of the schools needs to be determined. Only if schools make cybersafety a priority, will teachers follow.

Cybersafety maturity of schools is vital to ensuring that an environment where learners can be cyber safe is provided, thus contributing to a national cybersafety culture. Schools have a social responsibility to ensure that learners have the necessary awareness, knowledge and skills regarding cybersafety [14,30]. Preparing school learners for the 4th Industrial Revolution includes preparing them for interacting with cyberspace and other cyber users safely and securely [31]. By measuring maturity, this research explored how schools in South Africa can facilitate social change among school learners with regard to cyber activities such as cyberbullying and exposure to inappropriate material.

According to Vishwanath et al. [32], measuring cyber-related issues is still not receiving sufficient attention within cyber communities. Social change within cybersafety behaviour should be a top-down approach [33]. This includes management's responsibility in terms of leadership, policies and awareness education to ensure that cybersafety change is driven through proper management support and commitment. The current research culminated in a proposed ten-phase process to guide schools with low cybersafety maturity to increase and grow a cybersafety culture to support their learners and teachers.

3. Methodology and Data-Gathering Method

This research study follows an inductive approach, and consists of three research methods. Research method one is based on a literature review that investigates the current situation regarding cybersafety maturity within school environments (Section 2 of the article). Method two includes the three steps of data gathering, data analysis and the feedback of findings (Section 4 of the article). This is a quantitative data-gathering approach with the underlining principle of gathering data until saturation point has been reached. Full ethical clearance was obtained through the University of South Africa to conduct the research study. An existing survey tool, 360safe, which is an online safety review tool, was used. This tool is freely available online at https://360safe.org.uk/. Full permission was obtained from Childnet, London, UK to use this tool for gathering data within the South African environment. The 360safe tool includes the maturity of cybersafety within the four element areas of policy and leadership, infrastructure, education and standards, and inspection. Each one of the elements is further divided into different strands that support each element. Each strand can have one or more actions linked to different strands. Table 1 depicts the elements, strands and actions to measure cybersafety within a school environment.

Table 1. 360safe online safety review tool (obtained from http://360safe.org.uk).

Element A: Policy and Leadership		
Strand 1: Responsibility		
A1.1.	Online safety group	This aspect describes how the school manages its online safety strategy involving a group with wide-ranging representation.
A1.2.	Online safety responsibilities	This aspect describes the roles of those responsible for the school's online safety strategy.
A1.3.	Governors	This aspect describes the online safety accountabilities of the school's Board of Directors, and how the school ensures this influences policy.
Strand 2: Policies		
A2.1.	Policy development	This aspect describes the process of establishing an effective online safety policy involving the stakeholders and their responsibilities, consultation, communication, review and impact.
A2.2.	Policy scope	This aspect considers policy content, its breadth in terms of technology and expectations around behaviour, and its relevance to current social trends and educational developments.
A2.3.	Acceptable use	This aspect considers how the school communicates its expectations regarding acceptable use of technology and the steps towards successfully implementing these expectations within the school.
A2.4.	Self-evaluation	This aspect describes how the online safety self-evaluation process builds upon and aligns with other self-evaluation mechanisms.
A2.5.	Whole school	This aspect describes how the online safety policy is consistent with school expectations in other relevant policies/safeguarding practices and vice versa (e.g., behaviour, anti-bullying and preventative action plans).
A2.6.	Managing unacceptable use	This aspect considers the actions the school may take and the strategies it employs in response to misuse. There is evidence that responsible use is acknowledged through celebration and reward.
A2.7.	Reporting	This aspect describes the routes and mechanisms the school provides for its community to report abuse and misuse.
Strand 3: Communications and communications technology		
A3.1.	Mobile technology	This aspect considers the benefits and challenges of mobile technologies, and their use in a school environment and beyond.
A3.2.	Social media	This aspect covers the use of social media in and by the school and where appropriate, beyond the school. It considers how the school can educate all users about the responsible use of social media.
A3.3.	Digital and video images	This aspect describes how the school manages the use and publication of digital and video images in relation to the requirements of the data protection act.
A3.4.	Public online communications	This aspect describes how the school manages its public-facing online communications in both managing risk, and disseminating online safety advice, information and practice.
A3.5.	Professional standards	This aspect describes how staff's use of technology complies with both school policy and professional standards.

Table 1. *Cont.*

Element B: Infrastructure		
Strand 1: Passwords		
B1.1.	Password security	This aspect covers the ability of the school to ensure the security of its systems and data through good password policy and practice.
Strand 2: Services		
B2.1.	Filtering and monitoring	This aspect describes how the online safety policy is consistent with school expectations in other relevant policies/safeguarding practices.
B2.2.	Technical security	This aspect describes the ability of the school to understand and ensure reasonable duty of care regarding the technical and physical security of administrative and curriculum networks.
B2.3.	Data protection	This aspect describes the ability of the school to be compliant with the current Protection of Personal Information Act. Note this section was adapted to the POPI Act within South Africa (No 4 of 2013).
Element C: Education		
Strand 1: Children and young people		
C1.1.	Online safety education	This aspect describes how the school builds resilience in its learners/students through an effective online safety education program.
C1.2.	Digitalliteracy	This aspect describes how the school develops the ability of young people to find, evaluate, use, share and create digital content in a way that minimises risk and promotes positive outcomes.
C1.3.	Contribution of young people	This aspect describes how the school maximises the potential of young people's knowledge and skills in shaping an online safety strategy for the school.
Strand 2: Staff		
C2.1.	Staff training	This aspect describes the effectiveness of the school's online safety development programme for staff, and how it prepares and empowers staff to educate and to intervene in issues when they arise.
Strand 3: Governors		
C3.1.	Governor education	This aspect describes the school's provision of online safety education for governors (Board of Directors) to support them in the execution of their roles.
Strand 4: Parents and carers		
C4.1.	Parental engagement	This aspect describes how the school educates and informs parents and carers on issues relating to online safety, including support in establishing effective online safety strategies for the family.
Strand 5: Community		
C5.1.	Community engagement	This aspect describes how the school communicates and shares best practices with the wider community, including local people, agencies and organisations.
Element D: Standards and inspection		
Strand 1: Monitoring		
D1.1.	Monitoring and reporting safety incidents	This aspect covers the school's effectiveness in monitoring and recording online safety incidents, including its response to such incidents and how the online safety strategy is informed.
D1.2.	Online safety policy and practices	This aspect covers the effectiveness of the school's online safety strategy, the evidence used to evaluate impact, and how such evidence shapes developments in policy and practice.

The UK 360safe measuring tool indicated in Table 1 was used to determine the cybersafety maturity of schools, which was investigated in view of the different elements, strands and aspects. Each aspect was evaluated against five levels of a maturity scale. This five-point maturity scale ranged from Level 5, indicating no adherence to the elements, strands and aspects, to Level 1, indicating full adherence to the elements, strands and aspects. Schools therefore should strive to comply with Level 1 for maturity regarding each element, strand and aspect.

The online tool (survey approach) was used to obtain current information from 24 South African schools. In South Africa, the Living Standards Measure (LSM) represents a segmentation tool that is used to understand the market based on access to services and durables, together with geographic indicators as determinants of standards of living. The 24 schools investigated in the current study consisted of 27% private schools and 73% public schools. This representation was determined according to the South African division of private and public schools in which 20% of the schools are classified

as LSM 3–5 schools and 80% as LSM 6–9 schools. The lower LSM schools in this sample represented the emerging market, and the higher LSM schools represented the established market. Furthermore, of the 24 schools, 63% were high schools, 28% were primary schools and 14% were combined schools (primary and high school). The data analysis from the 24 schools showed that the saturation point had been reached and no further data needed to be gathered. However, it is noted that this can be a shortcoming of the research. In Section 6 it is suggested that this study (without the saturation clause) be conducted among all schools within South Africa to obtain a national viewpoint of cybersafety maturity within schools.

The last method includes the proposal of a theoretical framework based on the findings of the data analysis as well as the literature review process (Section 5 of the article).

4. Data Analysis

The data from the survey was analysed statistically and findings were made based on the analysis. Cronbach's alpha, which measures internal consistency and estimates the reliability of test scores for the survey, was calculated at 0.95 and indicated that the findings were internally consistent and reliable. It should be noted that the findings of the data analysis indicated a clear variation between private and public schools. Little variation or data deviation was found between high schools and primary schools, or between lower and higher LSM schools. For each aspect, the results are given for the private and the public schools in addition to the overall average for both the public and the private schools. Each of the four elements is discussed separately.

4.1. Element A: Policies and Leadership

This involves the maturity of the aspects within the three strands (responsibility, policies and communications) that measured policies and leadership (Element A) within each school. The results are depicted in Figure 1 and indicate the findings for public and private schools, and the average for both. The findings are plotted on a scale of 1 to 5 (1 is compliance with cybersafety and 5 is the lack thereof).

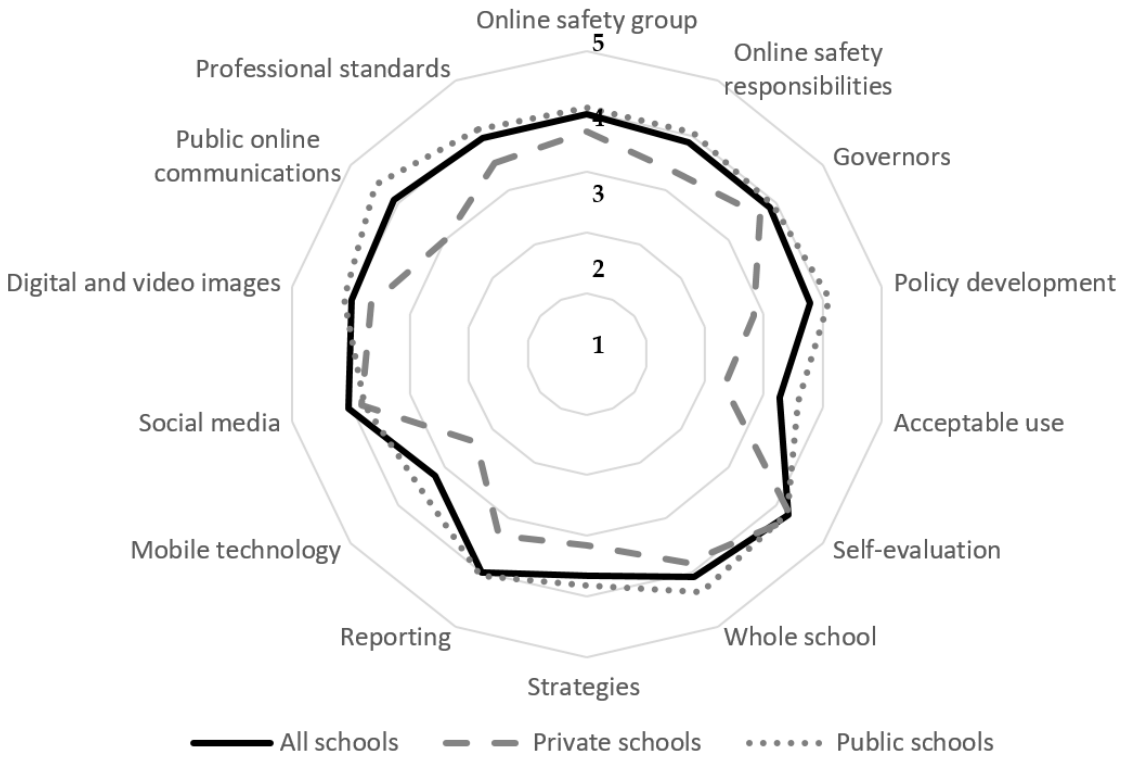

Figure 1. Strands 1, 2 and 3 of Element A.

From the statistics depicted in Figure 1, the maturity within all the schools is extremely low. The findings indicate that maturity in the private schools is better than in the public schools, but in most cases a score higher than 3 was obtained. The average for all the schools (barring the acceptable-use aspect) is higher than 3.5. It is evident that the private schools scored slightly higher for maturity than the public schools due to extra funding being available.

4.2. Element B: Infrastructure

This involved the maturity of the aspects within the two strands (passwords and services) that measured the infrastructure (Element B) within each school. The four aspects that were measured were password security, filtering and monitoring, technical security and data protection. The results are depicted in Figure 2.

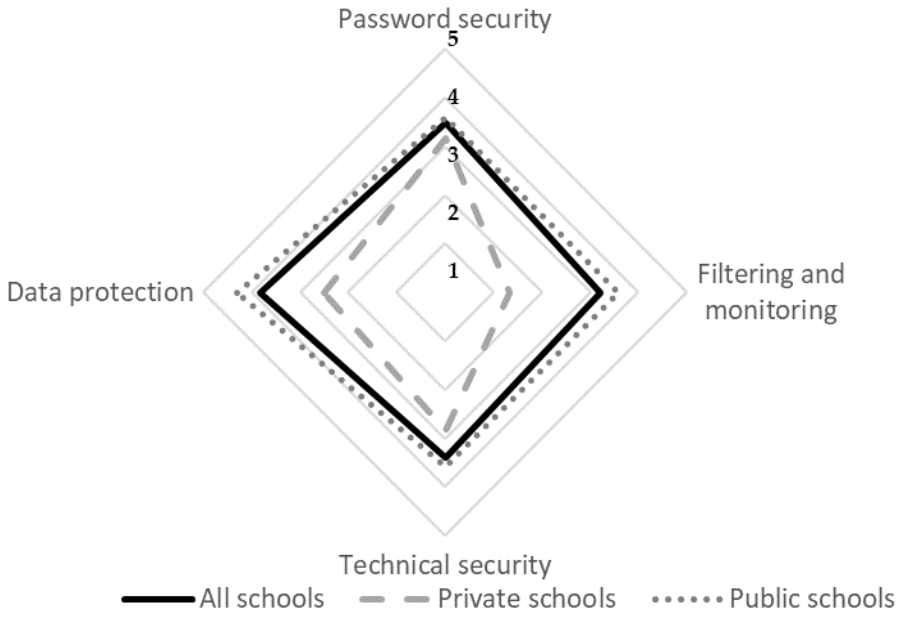

Figure 2. Strands 1 and 2 of Element B.

Figure 2 depicts the results of Element B regarding infrastructure. Once again, private schools scored better than public schools in all four aspects. One aspect that raised concern was data protection. According to the South African Protection of Personal Information Act 4 of 2013, schools must ensure that all learners' data is properly protected. This is currently not being done in either the private schools or the public schools.

4.3. Element C: Education

This involved the maturity of the aspects within the five strands (children and young people; staff; governors, parents and careers; parental engagement; and community engagement) within Element C, which measures the education element within each school. The aspects that were measured were online safety, digital literacy, contribution of young people, staff training, governor education, parental engagement and community engagement.

The overall findings indicate that all the schools (public and private) scored the lowest for this element compared with the other elements. Online safety (aspect C1.1.) scored an average of 4.5, governor education (C3.1.) scored an average of 4.1, and parental engagement (C4.1.) and staff training (C2.1.) scored just below 4.5.

From the data analysis, it is clear that within all the schools that took part in the research study, education (including staff training) on cybersafety ranks the lowest, with minimum input from either the school or government. The results are depicted in Figure 3.

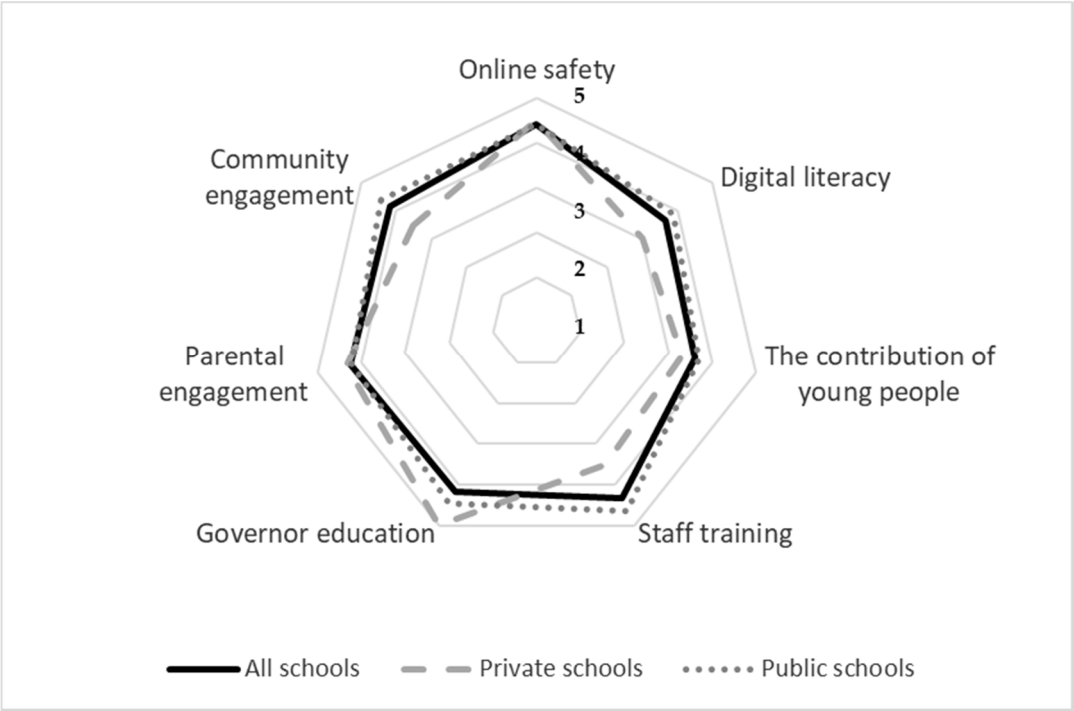

Figure 3. Strands 1 to 5 of Element C.

4.4. Element D: Standards and Inspection

Element D involved the maturity of the aspects within the strand of monitoring, which measured the standards and inspection (Element D) within each school. The results are depicted in Figure 4.

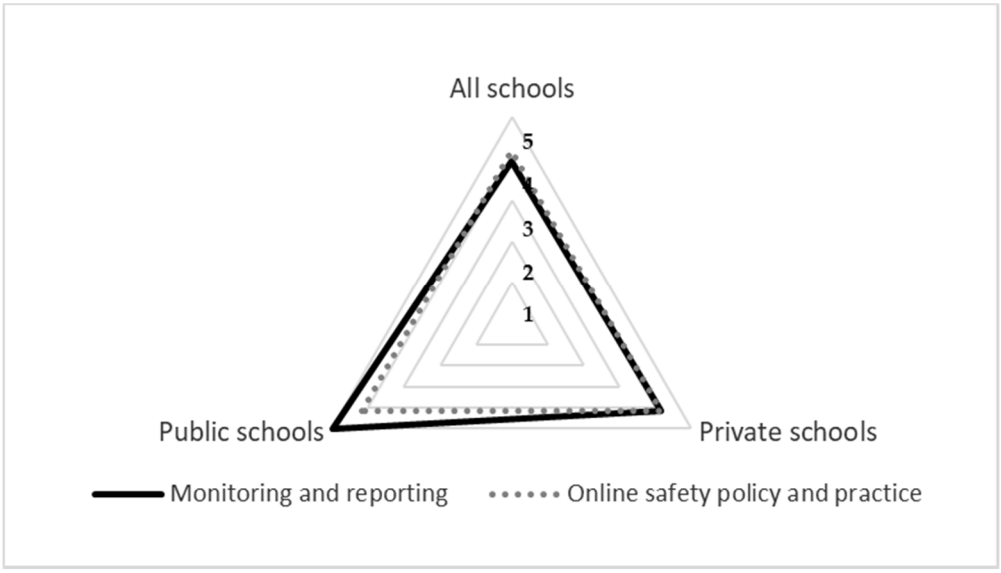

Figure 4. Strand 1 of Element D.

This element scored an average of 4 for both aspects. This is a warning sign that in both private and public schools the aspects of measuring and monitoring are lacking and require urgent attention.

4.5. Discussion of Overall Findings

The discussion focuses on the results of the maturity evaluation to provide an overview of the current cybersafety maturity of South African schools. The overall findings focus on the four main

elements, namely policies and leadership, infrastructure, education, and standards and inspection. Ideally, the cybersafety maturity of schools should be at Level 1. Level 1 indicates that cybersafety measures are aspirational and innovative, and that there is full compliance. The long-term goal is for all schools within South Africa to comply with Level 1.

The Level 5 scores indicate that there is little or nothing in place within the school to ensure the cybersafety of the learners. The results also provide some insight into the involvement and practical implementation of changing the social cybersafety culture within the given schools. Currently, a social cybersafety culture is not being created and grown. Figure 5 depicts the overall scores for the four elements from both the public and private schools, and the averages for both.

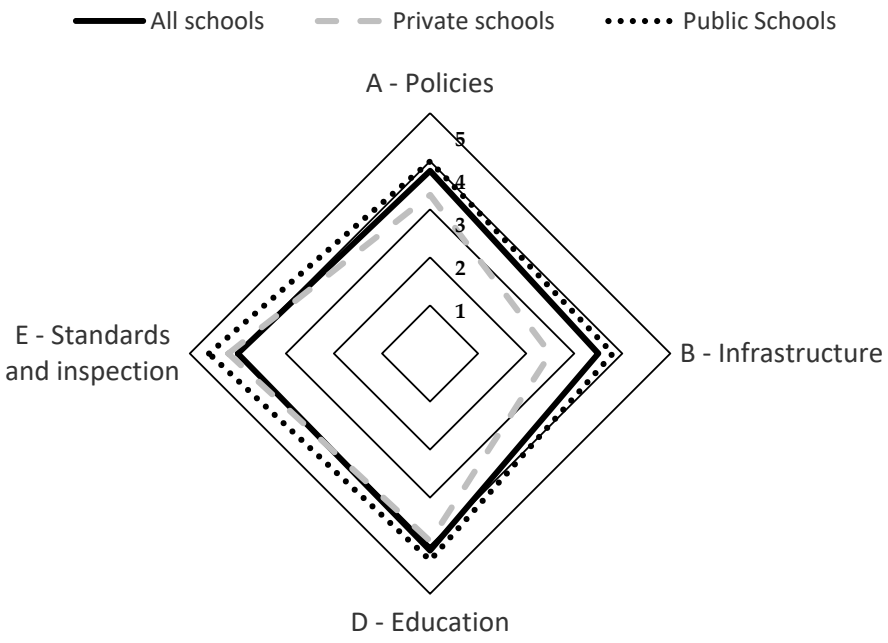

Figure 5. Overview of averages of all four elements.

Figure 5 demonstrates that in most instances, private schools are slightly more mature than public schools. However, this is only by a small margin and only in a few aspects. Private schools had an average maturity span of 3.5 to 4, whereas the public schools scored mostly between 4 and 5. In both public and private schools, the scoring was very high, approaching non-compliance. This indicated very low cybersafety maturity in all the aspects that were measured. From the data analysis, the following strengths were identified:

- Filtering and monitoring (3.2)
- Acceptable-use policies (3.3)
- Technical security (3.4)

The results indicated that these strengths were aspects that were being addressed within the schools. However, all three strengths demonstrated a maturity level of more than 3, which indicated that much improvement is still needed. The four identified weaknesses scored above 4.3. These weaknesses are as follows:

- Staff training (4.3)
- Parental engagement (4.3)
- Online safety (4.4)
- Data protection (4.3)

It should be noted that three of the top four weaknesses are within the element of education of all the different stakeholders, which includes parents, teachers and the learners themselves. The fourth weakness, data protection, is alarming and requires urgent attention in view of the Protection of Personal Information Act 4 of 2013—POPI legislation) in South Africa. This will force schools to ensure that the data of learners is protected properly.

The findings of the study also indicated that a number of schools have access to technology that forms part of the school's infrastructure (as depicted in Figure 5 that indicates an average score of 2.5 for infrastructure). This means that schools are starting to add technology as an educational method to prepare learners for a technological future. However, the findings indicate that schools are not supporting the required policies, education and monitoring tools to establish healthy social and educational interaction with technology.

It is critical that a holistic approach is implemented when focusing on the four elements of cybersafety maturity. The results demonstrate that all the schools (private and public) scored between 3 and 5 for almost all elements. This indicates that schools within South Africa have a low cybersafety maturity. This critical problem requires drastic and immediate attention from a managerial stance. The analysis indicates that possible factors influencing the current maturity levels within South African schools are the lack of a number of cyber-related issues. These issues (within a South African context) are included in the list below:

- cybersafety knowledge and skills [34]
- funding to create cybersafety materials [35,36]
- motivation to establish and grow a cybersafety culture [28]
- leadership to ensure that the necessary cybersafety measures are in place
- commitment by parents/guardians to become involved in cybersafety education
- participation by learners [37]
- guidance by government (Department of Basic Education) [29,38]
- training opportunities for school teachers [28]
- school material (e.g., curriculum) [27]
- cybersafety policies and procedures at the government level [27]
- cybersafety policies and procedures for schools [29,39]
- a monitoring and reporting system [40]
- social support for cyber victims in schools [41]
- national guidance and assistance [27,42]
- planning documents

The critical aspect identified through this research is that there is almost no assistance or guidance from the South African government (Department of Basic Education) towards improving cybersafety within schools. There are no cybersafety policies and procedures provided for the schools to implement, no evaluation system to ensure that schools comply and no monitoring to evaluate if progress is being made. Despite many schools in South Africa attempting (even in some small way) to improve cybersafety, without the intervention of government and the Department of Basic Education, any attempts will be in silos. Ideally, this should be a top-down approach that begins with government and the Department of Basic Education [27,33,43,44]. This should be followed closely with the buy-in from school boards, teachers, parents and school learners.

The measuring tool can be used as a first step to indicate the cybersafety elements and aspects that should be in place to establish, grow and cultivate a cybersafety culture within schools. It is clear from this research that a national educational framework is needed to address all the required cybersafety aspects in order to bring cybersafety to the fore within the education environment.

However, until government and the education department recognise their role and responsibility regarding cybersafety within schools, schools should proceed on their own to establish and grow a

cybersafety culture. This means that social responsibility regarding cybersafety defaults to the school and the governing body of the school.

5. Proposed Cybersafety Maturity Guidelines for South Africa

This research proposes a step-by-step guideline with a ten-step phased approach that schools can adopt to provide an environment in which a cybersafety culture can be established, implemented and cultivated. The guidelines are underlined by three steps: Plan, Action and Evaluate.

The first step includes the phases that are involved in the planning of actions and initiatives to improve cybersafety. The second step involves the implementation of the different phases to ensure that the plan is executed according to the planning phases. The last step entails evaluation to ensure that the implementation of the plan has contributed to increased cybersafety within the school. Each step consists of a number of phases. The research identified ten phases that encompass the cyber issues identified as "currently lacking" in South Africa. Each of the ten phases is allocated to one of three steps as indicated in Figure 6.

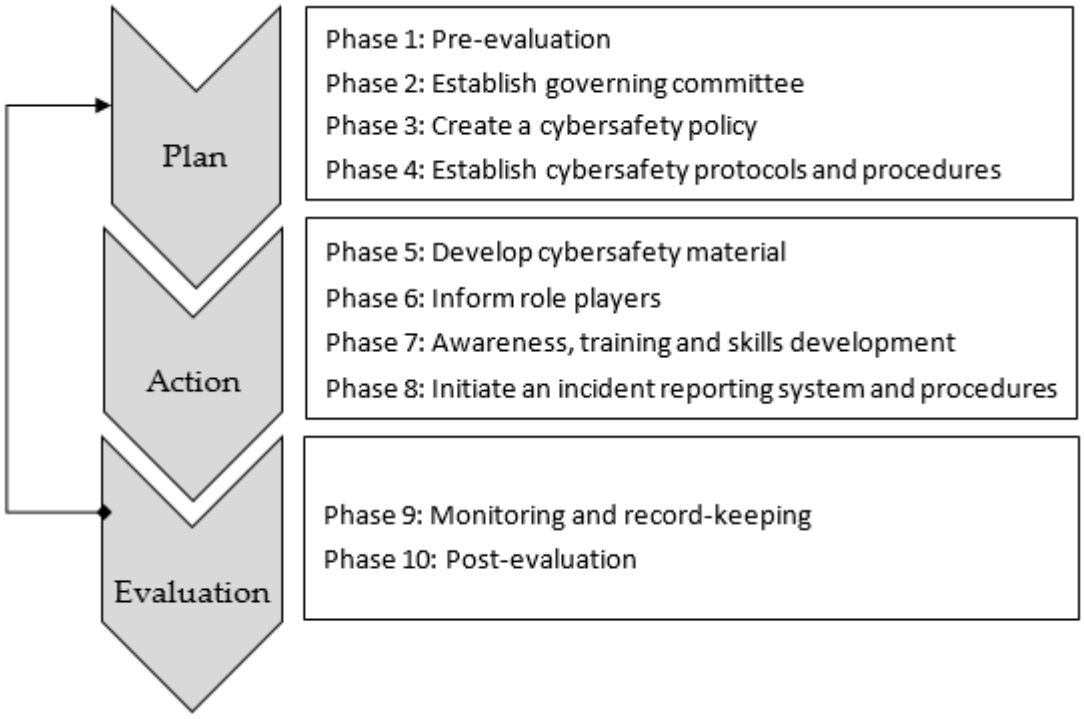

Figure 6. Ten-phase approach to cybersafety awareness.

Each of the ten phases has a number of actions that are linked to the phase. Phase 1 addresses pre-evaluation and focuses on evaluating the current cybersafety environment within a school. This phase includes obtaining a baseline for existing awareness, knowledge and skills among teachers and learners, and establishing the current cybersafety resources within the school. These resources include available funding and equipment, access to technology, and current cybersafety culture. Phase 2 focuses on establishing the governing committee. The school should establish a cybersafety committee with a wide range of representatives. The committee should include the school's governing body (SGB) and representatives comprising teachers, parents and external advisers who include legal personnel, social worker(s) and active member(s) of the police force.

Phase 3 aims to establish a cybersafety policy within the school. The school's cybersafety awareness policy should be linked and in line with existing policies that include a technology policy, an acceptable-use policy, a communication policy and a risk-management policy. Each school has the flexibility to align the cybersafety policy with the school's environment, and this may differ from other

schools. Phase 4 focuses on establishing cybersafety protocols and procedures. This phase uses the cybersafety policy to create protocols and procedures for implementing the policy.

Phase 5 includes the development of cybersafety material and related initiatives. The development of material and initiatives depends on the funding, resources and time available within the calendar of each school. Phase 5 also differentiates between using existing documents and resources, and developing documents and resources specifically for the school. South Africa has 11 official languages, and developing relevant documents in a specific language may be an issue. Phases 5 and 6 are the only phases that can proceed in parallel; all the other phases are implemented in series (one after the other). Phase 6 focuses on informing all role players of their roles and responsibilities towards the cybersafety policy. All role players must understand the rules set out in the cybersafety policy, and the consequences if the policy is not observed.

Phase 7 is part of the implementation step and focuses on delivering the developed/adopted cybersafety material and initiatives to the role players, who include the teachers, learners and parents/caregivers. Phase 8 ensures that the incident-reporting aspect of the cybersafety policy is implemented and enforced. All role players must be made aware of the process used to report incidents in a safe way.

Phase 9 addresses the process of implementing the cybersafety policy. Record-keeping must be done correctly to ensure evidence is kept, all open cases are addressed and the results of closed cases are properly reported. The last phase, Phase 10, is the post-evaluation process to determine if the cybersafety policy was implemented correctly, if the awareness, knowledge and skills increased among the role players, and if the reported cases were addressed properly. Depending on the outcome of the post-evaluation, the cybersafety policy can be amended.

Each of the ten phases can be further subdivided into specific guidelines (actions) on how to implement the phase. The ten phases and the identified guidelines within each phase are depicted in Table 2.

Table 2. Ten-phase approach to cybersafety.

	Phase 1: Pre-Evaluation
1.1.	Delineate existing/prior knowledge and skills of learners and teachers
1.2.	Identify funding and resources available for cybersafety activities
1.3.	Determine teachers' and learners' access to technology
1.4.	Determine current cybersafety culture within the school
1.5.	Evaluate existing cybersafety material
	Phase 2: Establish Governing Committee
2.1.	Establish the cybersafety committee (part of the ICT committee)
2.2.	Identify the school's responsiveness towards cybersafety
2.3.	Establish management protocols and governance procedures
2.4.	Assign management committee responsibilities
2.5.	Initiate a consultation process with representatives from the Department of Education
2.6.	Consult with legal representation
2.7.	Identify risk factors for risk register
2.8.	Identify success indicators
	Phase 3: Create a Cybersafety Policy
3.1.	Design a cybersafety policy/acceptable-use policy (AUP) (or adapt existing document)
3.2.	Create protocol for supporting structure related to cyber incidents

Table 2. *Cont.*

Phase 4: Establish Cybersafety Protocols and Procedures to Support Policy	
4.1.	Infrastructure
4.2.	Education (awareness, training and skills development)
4.3.	Implementation process
4.4.	Reporting
4.5.	Monitoring and measuring
4.6.	Pre-evaluation
Phase 5: Develop Cybersafety Material	
5.1.	Identify role players and their responsibility for developing material
5.2.	Initiate consultation process with designing team
5.3.	Identify training programs for teachers
Phase 6: Inform Role Players	
6.1.	Consultation process with external role players
6.2.	Consultation process with teachers
6.3.	Consultation process with parents
6.4.	Consultation process with learners
Phase 7: Awareness, Training and Skills Development	
7.1.	Increase knowledge and skills of teacher
7.2.	Improve awareness of learner
7.3.	Advise parents and care givers
Phase 8: Incident-Reporting System and Procedures	
8.1.	Implement reporting system and procedures
8.2.	Inform all role players of process regarding the reporting of incidents
Phase 9: Monitoring and Record-Keeping	
9.1.	Implement monitoring process
9.2.	Implement record-keeping process
9.3.	Identify the audit process of monitoring and record-keeping
9.4.	Establish reported process
Phase 10: Post-Evaluation	
10.1.	Evaluate/measure success indicators
10.2.	Revise policies

These ten phases are closely linked to the maturity elements that were measured in this research study and depicted in Table 1. However, additional phases were added to provide schools with a holistic, step-by-step approach to implementing cybersafety. The ten phases and the actions of each phase can guide schools in initiating the process to address cybersafety within schools. Figure 7 depicts an overview of the phases (processes/actions) that a school can follow to create and implement a safe cyber environment.

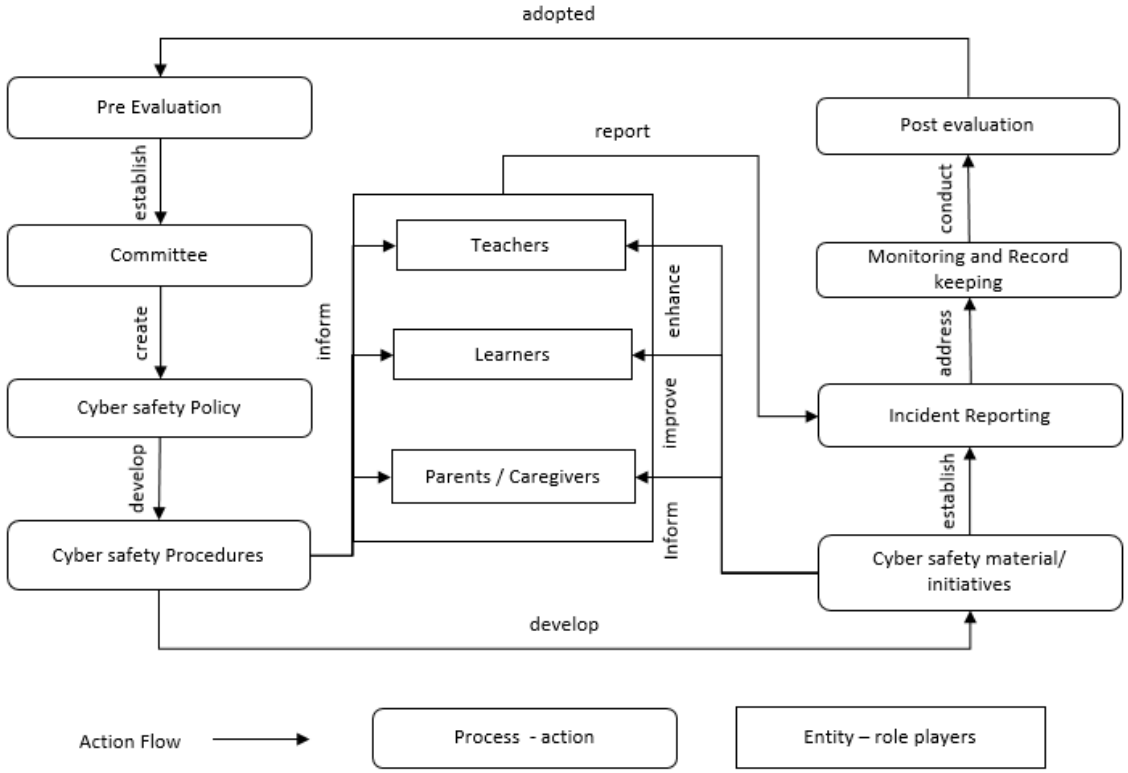

Figure 7. Flow diagram of cybersafety implementation.

Figure 7 presents the phases as a step-by-step process that indicates the order of the processes and the linking to the entities (role players). For example, the cybersafety procedures will depend on the cybersafety policy. It is, therefore, vital that the phases are carried out in the correct sequence, with only Phases 5 and 6 occurring concurrently. The last phase completes the loop by linking to step 3 (cybersafety policy) to ensure continuous evaluation and to ensure that the cybersafety policy is updated where needed. It is vital to note that creating a cybersafety culture is dependent on each phase being implemented holistically in relation to the other phases. If one phase is omitted, the holistic approach to a coherent cyber culture will be compromised. It is strongly advised that all schools adhere to all the phases. However, due to workload, knowledge and skills as well as financial considerations, the depth of implementation will differ among schools. The depth of the implementation will be pinpointed in Phase 1, which includes a pre-evaluation to determine the resources available that can be used in the other phases of implementation.

Ultimately, this approach to create a cybersafety culture within schools should be guided, driven and sustained by government. However, until schools are fully supported by government, they should take the mandate upon themselves to ensure their learners and teachers are cyber safe. It is strongly advised that the implementation of a cybersafety strategic plan (upon the proposed cybersafety guidelines) is completed as soon as the needed resources allow (short-term approach). Additional cybersafety measures can be implemented or approved as resources become available (long-term approach). The proposed guidelines provide schools with a sense of direction and a step-by-step plan to establish, grow, and cultivate a cybersafety environment for learners and teachers to create their own cybersafety culture.

6. Conclusions

The maturity of cybersafety within South African schools was investigated by means of an empirical study. The study used a UK-approved maturity tool to evaluate four main elements of cybersafety compliance: leadership and polices, infrastructure, education, and standards and inspection,

with each element having a number of sub-actions. The results of the study showed that both private and public schools have very low maturity regarding cybersafety within all four elements. Most elements scored between 3 and 5, except for a few elements in public schools. The analysis indicates that education is an aspect that requires the most attention, and government and management should place it in the foreground to ensure a cybersafety culture within South African schools. In addition, the analysis found that schools do not have a step-by-step process for creating, growing and cultivating a cybersafe environment for school learners. The research proposed an action flow process consisting of ten phases and actions that a school can implement to cultivate a cybersafety culture.

The future direction of the research will include conducting a study to find out why private schools are a bit more prepared to create a cyber culture. Future research can also include the comparison between the maturity of schools and higher education (universities). One limitation of the research is that the proposed guidelines were not tested and validated. This will be part of the future research.

The paper suggested that the funding of private schools is the driver behind the preparedness, but this will be determined in another round of data gathering. The research will also attempt to provide a peer-to-peer guideline to enhance cybersafety awareness among learners (learners teaching each other). This approach will focus on the learners themselves creating and growing the cybersafety culture within the school, and the teachers being only the facilitators.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Barbosa, J. How to Educate to Build an Effective Cyber Resilient Society. *Int. J. Cyber Res. Educ.* **2020**, *2*, 55–72. [CrossRef]
2. Randa, R. The in fluence of the cyber-social environment on fear of victimization: Cyberbullying and school. *Secur. J.* **2013**, *26*, 331–348. [CrossRef]
3. Alotaib, F. *Evaluation and Enhancement of Public Cyber Security Awareness*; Unversity of Plymouth: Plymouth, UK, 2019.
4. De Lange, M. *Guidelines to Establish an e-Safety Awareness in South Africa*; Nelson Mandela Metropolitan University: Port Elizabeth, South Africa, 2012.
5. International Telecommunication Union. Global Cybersecurity Index (GCI) 2017. ITU-D Global, 2017. Available online: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (accessed on 2 September 2020).
6. Castilla, J.E.M.; Pursiainen, C. Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not? *J. Civ. Soc.* **2019**, *15*, 392–411. [CrossRef]
7. Wright, M.F. Adolescents' cyber aggression perpetration and cyber victimization: The longitudinal associations with school functioning. *Soc. Psychol. Educ.* **2015**, *18*, 653–666. [CrossRef]
8. Rahman, A.; Malaysia, N.A.; Sairi, M.T.U.K.; Zizi, I.K.; Khalid, F. The Importance of Cybersecurity Education in School. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 378–382. [CrossRef]
9. DePaolis, K.; Williford, A. The Nature and Prevalence of Cyber Victimization among Elementary School Children. *Child Youth Care Forum* **2014**, *44*, 377–393. [CrossRef]
10. De Barros, M.J.Z.; Lazarek, H. A Cyber Safety Model for Schools in Mozambique. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal, 22–24 January 2018; Scitepress: Setúbal, Portugal, 2018; pp. 251–258.
11. Shariff, S.; Hoff, D.L. Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace. *Int. J. Cyber Criminol.* **2007**, *1*, 76–118.
12. Pencheva, D.; Hallett, J.; Rashid, A. Bringing Cyber to School: Integrating Cybersecurity into Secondary School Education. *IEEE Secur. Priv. Mag.* **2020**, *18*, 68–74. [CrossRef]
13. Abawajy, J.H. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2012**, *33*, 237–248. [CrossRef]

14. Dlamini, Z.; Modise, M. Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. In Proceedings of the 7th International Conference on Information Warfare and Security, Seattle, DC, USA, 22–23 March 2012; pp. 98–107.
15. Smith, C. *Cyber Security, Safety and Ethics Education*; Utica College, ProQuest Publishing: Emeryville, CA, USA, 2018.
16. Kritzinger, E. Cultivating a cyber-safety culture among school learners in South Africa cultivating a cybersafety culture. *Afr. Educ. Rev.* **2017**, *14*, 22–41. [CrossRef]
17. Antoniadou, N.; Kokkinos, C. Cyber and school bullying: Same or different phenomena? *Aggress. Violent Behav.* **2015**, *25*, 363–372. [CrossRef]
18. Gonzales, R.H. Social Media as a Channel and its Implications on Cyber Bullying. In Proceedings of the DLSU Research Congress, Manila, PH, USA, 20–22 June 2006; pp. 1–7.
19. Von Solms, S.; Von Solms, R. Towards Cyber Safety Education in Primary Schools in Africa. In Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), Plymouth, UK, 8–9 July 2014; pp. 185–197.
20. Peterson, J.; Densley, J. Cyber violence: What do we know and where do we go from here? *Aggress. Violent Behav.* **2017**, *34*, 193–200. [CrossRef]
21. Edwards, S.; Nolan, A.; Henderson, M.; Mantilla, A.; Plowman, L.; Skouteris, H. Young children' s everyday concepts of the internet: A platform for cyber-safety education in the early years. *Br. J. Educ. Technol.* **2018**, *49*, 45–55. [CrossRef]
22. Zwilling, M.; Lesjak, D.; Natek, S.; Phusavat, K.; Anussornnitisarn, P. How to Deal with the Awareness of Cyber Hazards and Security in (Higher) Education? Thriving on Future Education, Industry, Business and Society. In Proceedings of the MakeLearn and TIIM International Conference, Piran, Slovenia, 15–17 May 2019; pp. 433–439.
23. Kritzinger, E.; Bada, M.; Nurse, J. A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In Proceedings of the WISE 10 (IFIP), Shangai, China, 8–10 November 2017; pp. 1–11.
24. Pelletier, R.; Handal, B.; Khalil, J.; Francis, T. Cyberbyllying-when does a school authority's liabilty in tort end? *West. Aust. Jurist.* **2015**, *6*, 93–121.
25. Srivastava, J.S. Cyber Crime: Kids as Soft Targets. *Int. J. Innov. Comput. Sci. Eng.* **2017**, *4*, 31–36.
26. Miles, D. Youth Protection. In Proceedings of the Cybersecurity Summit (WCS), London, UK, 1–2 June 2011; pp. 1–3.
27. Kortjan, N.; Von Solms, R. A conceptual framework for cyber security awareness and education in SA. *S. Afr. Comput. J.* **2014**, *52*, 29–41. [CrossRef]
28. Govender, I.; Skea, B. Teachers' Understanding of E-Safety: An Exploratory Case in KZN South Africa. *Electron. J. Inf. Syst. Dev. Ctries.* **2015**, *70*, 1–17. [CrossRef]
29. Cilliers, L.; Chinyamurindi, W.T. Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa. *Electron. J. Inf. Syst. Dev. Ctries.* **2020**, e12131. [CrossRef]
30. Scholtz, D.; Kritzinger, E.; Botha, A. Underpinning Knowledge and Skills for Educators to Enhance Cyber Safety Awareness in South African Schools. *Bioinform. Res. Appl.* **2019**, *11937*, 278–290. [CrossRef]
31. Kempen, A. The 4th Industrial Revolution. *Servamus* **2019**, *112*, 10–12.
32. Vishwanath, A.; Neo, L.S.; Goh, P.; Lee, S.; Khader, M.; Ong, G.; Chin, J. Cyber hygiene: The concept, its measure, and its initial tests. *Decis. Support. Syst.* **2020**, *128*, 113160. [CrossRef]
33. Von Solms, R.; Von Solms, S. Cyber Safety Education in Developing Countries. In Proceedings of the 9th International Multi-Conference on Society, Cybernetics and Informatics, Proceedings (IMSCI 2015), George, South Africa, 11–12 December 2015; pp. 173–178.
34. De Lange, M.; Von Solms, R. An e-Safety Educational Framework in South Africa. In Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC), George, South Africa, 2–5 September 2012.
35. Mashiane, T.; Dlamini, Z.; Mahlangu, T. A rollout strategy for cybersecurity awareness campaigns. In Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa, 28 February–1 March 2019; pp. 243–250.

36. Grobler, M.; Flowerday, S.; Von Solms, R.; Venter, H. Cyber Awareness Initiatives in South Africa: A National Perspective. In Proceedings of the First IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW) 2011, Gaborone, Botswana, 12 May 2011; pp. 32–41.
37. UNICEF. Your People's Navigation of Online Risks 2012. Available online: http://goo.gl/hqaXJ9 (accessed on 10 March 2014).
38. Grobler, M.; Dlamini, Z. Global Cyber Trends a South African Reality. In Proceedings of the IST-Africa 2012 Conference, Dar es Salaam, Dar es Salaam, Tanzania, 9–11 May 2012; pp. 1–8.
39. Kyobe, M.E.; Mimbi, L.; Nembandona, P.; Mtshazi, S. Mobile Bullying Among Rural South African Students: Examining the Applicability of Existing Theories. *Afr. J. Inf. Syst.* **2018**, *10*, 1.
40. Odora, R.J. The Nature and Prevalence of Cyber Bullying Behaviors among South African High School Learners. *Int. J. Educ. Sci.* **2015**, *10*, 399–409. [CrossRef]
41. Sonhera, N.; Kritzinger, E.; Loock, M. Cyber Threat Incident Handling Procedure for South African Schools. In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), Lesvos, Greece, 1–3 July 2015; pp. 215–232.
42. Bada, M.; Von Solms, B.; Agrafiotis, I. Reviewing National Cybersecurity Awareness in Africa: An Empirical Study. In Proceedings of the Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER 2018, Athens, Greece, 18–22 November 2018; pp. 78–83.
43. Vogel, R. Closing the Cybersecurity Skills Gap. *Salus. J.* **2016**, *4*, 32–46.
44. Kritzinger, E. Short-term initiatives for enhancing cyber-safety within South African schools. *S. Afr. Comput. J.* **2016**, *28*, 1–17. [CrossRef]

© 2020 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).