Eurasian Journal of Social Sciences, 9(3), 2021, 123-137
DOI: 10.15604/ejss.2021.09.03.001

EURASIAN JOURNAL OF SOCIAL SCIENCES

www.eurasianpublications.com

ROLES AND RESPONSIBILITIES FOR SCHOOL ROLE PLAYERS IN ADDRESSING CYBER INCIDENTS IN SOUTH AFRICA

Naume Sonhera
Corresponding Author: University of South Africa, South Africa
Email: 46329633@mylife.unisa.ac.za

Elmarie Kritzinger
University of South Africa, South Africa
Email: krize@unisa.ac.za

Marianne Loock
University of South Africa, South Africa
Email: Loockm@unisa.ac.za

Received: June 14, 2021 Accepted: August 24, 2021

Abstract

Cyber incidents are causing major challenges for school officials who are called upon to respond to these incidents involving learners, globally. Online threats take place off the radar screen of educators and parents, and this makes it difficult to address cyber incidents in schools and more impossible to monitor off school premises. The overwhelming challenges in South African schools are that there are no clear roles and responsibilities for relevant role-players when handling cyber incidents. Therefore, this article is aimed to determine the responsibilities of role players in handling cyber incidents in South African schools. The research used a qualitative approach and purposive sampling to collect data from the learners, to get their experiences and perceptions on reporting cyber incidents. The rationale for selecting learners was based on the view that cyber aggression is a very concerning issue in the school environment. The research went on to document the responsibilities of various role-players, which include the school with its educators, principal and the learners, the Department of Basic Education, the community, and the parents. The article focused on highlighting the roles and responsibilities of role players when handling cyber incidents in South African Schools and the views of learners on adults when handling cyber incidents. The study concludes that if the role players seriously follow their roles and responsibilities, cyber incidents can be reduced in schools. It is also important to note that role players cannot work in isolation; rather, they need a coordinated approach to share the responsibilities, as cyber incidents are not restricted to the classroom or school grounds. This problem requires all role players to work together, in proactive ways to intervene and reduce cyber incidents.

Keywords: Cyber, Incident, Learner, Victim, Aggressor, School, Responsibilities, South Africa, Role Player, Framework

1. Introduction

Cyber platforms proliferate in cyberspace, attracting learners in large numbers, globally, and posing the risk of them being subjected to cyber incidents. The cyber incident phenomenon is a concern for youth advocates, researchers, and the respective adults within and outside schools (Kowalski *et al.* 2019; Martin *et al.* 2018; Cross *et al.* 2006) Far from being limited to cyber victims, the effects of cyber incidents extend to the learners collectively, the school environment, and the entire school system (Astatke *et al.* 2021). The overwhelming challenges in South African schools are that there are no clear roles and responsibilities for relevant role-players when handling cyber incidents (Burton *et al.* 2016a). Learners are vulnerable in cyberspace and therefore need protection, help, and support from adults and other learners (Cilliers and Chinyamurindi, 2020; Government of Ireland, 2018). Learners from preschool through university represent a generation growing up with technology (McCoy and Lyons, 2018). McCoy and Lyons (2018) stated that technology has become a right to all learners, and this explains why it is used extensively throughout their daily lives, exceedingly how it is used by adults by a substantial margin (Bulger *et al.* 2017). The use of Information and Communication Technologies (ICTs) in South African Schools is also growing (Department of Basic Education, 2017). Learners are encouraged to surf through websites to view course material at their convenient time and location. While the awareness of the use of the Internet is growing among learners in South African schools, there is no increase in awareness of safe practices in the use of ICTs (Kritzinger, 2020). Learners receive mixed messages with regards to online behavior as they strive for technology literacy, sometimes without appropriate support (Myers and Cowie, 2019). Learners seem unaware of the risks of inappropriate behavior online, viewing them as trivial. South African learners are not immune to cyber incidents (Farhangpour *et al.* 2019).

In this study, cyber incidents are limited to instances that negatively impact learners and their educational environment. The researcher has defined the cyber incident as an act that violates cyber safety policy, computer safety policies or acceptable use of ICTs policies. As confirmed by Hellsten (2017), a cyber incident is any event that threatens, or impacts the cybersecurity, safety, confidentiality, or integrity of learners, or threatens the availability of electronic information of and for learners. Cyber incidents involve the intentional or negligent use of digital platforms or electronic media to cause harm to learners, impacts negatively on the education of learners, or create circumstances that are not conducive to teaching and learning. Because this article is focusing on youth in schools, the term ‘learner” is used to refer to individuals between 13 and 22 years.

In South African schools, there are no clear roles and responsibilities for relevant role-players when handling cyber incidents (Cilliers and Chinyamurindi, 2020; Bulger *et al.* 2017). The school staff members are not sure of what to do when learners are harassed online (Hills, 2017; Burton *et al.* 2016b). Limited research has been done to investigate how educators should handle cyber incidents (Phyfer *et al.* 2017). This has resulted in a lack of support from relevant role players in handling cyber incidents in schools (Kritzinger, 2020). Research that investigates South African learners’ perceptions on reporting cyber incidents is also virtually limited. Among South African educators, there is a gap between the desire to act and the confidence in the ability to effectively respond to cyber incidents. The reason being that educators are ill-equipped to deal with cyber incidents due to a lack of knowledge and skills, although there is an indication of high level of concern (Kritzinger, 2020). Currently, role players are not clear on their responsibilities when handling cyber incidents (Phyfer *et al.* 2017).

Researchers have found out that although cyber incidents often occur outside of school hours, the incidents regularly have an impact on learning and learning environments (Redmond *et al.* 2020; Myers and Cowie, 2019; Phyfer *et al.* 2017). Cyber incidents are also causing major challenges for school officials who are called upon to respond to cyber incidents involving learners (Redmond *et al.* 2020). Online threats take place off the radar screen of educators and parents, this makes it difficult to detect cyber incidents in schools and more impossible to monitor off school premises (Angus, 2016). Learners’ playgrounds have moved to social networks and due to the differences in generations, educators and parents do not always understand this new cyber world (Meier, 2021). The language that the learners use on the Internet has evolved and this has created a generation gap between learners and the adults around them. This enables learners to participate in cyber incidents without the fear of being discovered by adults (Astatke *et al.* 2021). The literature states that schools should have cyber incident reporting procedures and all cyber incidents among learners should be investigated, but no further information is provided on how this must be done and who is responsible for what. This study, therefore, seeks to understand how the identified role players can assist in handling cyber incidents in South African schools, that is, to determine the responsibilities of role players in the intervention during cyber incidents. The research article is guided by the following research question: To what extent are role players responding to cyber incidents in schools, and what are their responsibilities in the intervention during cyber incidents? The rest of the document is structured as follows, Section 2 explains the education sector in South Africa, Section 3 gives the literature review. The methodology is in Section 4 while the discussion of results is in Section 5. Section 6 explains the needs of role players; Section 7 gives the learners' perceptions about adults on issues of cyber incidents. Finally, Section 8 presents the conclusion and policy recommendations.

2. Education sector in South Africa

In South Africa, there are two departments, the Department of Basic Education (DBE) and the Department of Higher Education and Training (DHET) (Mhlanga, 2020). Primary and secondary education is directly controlled by the DBE, where public schools, private schools, Early Childhood Development centres (ECD) and special needs schools are looked after (Mhlanga and Moloi, 2020). The university education is controlled by the DHET, this includes the Vocational Education Training colleges (TVET), Adult Basic Education and Training (ABET) centers as well as Higher Education institutions (HE) (Department of Basic Education, 2018). Every province in South Africa has its education department, which is directly responsible for the implementation of policies crafted by the national department. These departments are also there to deal with local issues that are related to the execution of the mandate of the department at the national level.

As of 2016, the DHE reported that there were 29,749 public and registered independent schools in South Africa (Department of Basic Education, 2018). The number of ordinary schools was 25,574 while 4,175 were other educational institutions such as special schools and Early Childhood Development centers (ECD) (Department of Basic Education, 2018). The DBE also reported that the total number of educators were 425,000 in 2012 and 440,151 in 2016 who were reporting to the national department and the provincial department in the 9 provinces and the 86 districts of South Africa (South African Market Access, 2020). District and provincial DBE offices in nine provinces and 86 districts administer all the schools and have considerable influence over the implementation of policy (Department of Basic Education, 2018). The goals of the DBE and its district and provincial offices are to improve the quality of teaching, undertake regular assessments, improve on the Early Childhood Development, to ensure a system of outcomes-focused accountability (Mhlanga, 2020; Department of Basic Education, 2018).

The national curriculum statement of grade R to grade 12 expresses the knowledge, skills and values that are worth to be learned in schools in the country (Department of Basic Education, 2018). The goal of the curriculum is to make sure that the learners can acquire and apply the knowledge and skills in circumstances that prove to be meaningful to their own lives. Though the curriculum is sensitive to global imperatives, its main goal is to promote knowledge in the local context.

The DBE has many role-players which include the provincial departments of education, the district offices/officers, Council of education ministers, Heads of education departments committee, Umalusi, National education evaluation and development unit. Education labor relations council, South African council for educators, Educator unions and the school governing bodies are also part of the DBE role-players (Department of Basic Education, 2018).

The Department of Basic Education works closely with the provincial department to make sure that the provincial strategies and budgets are in line and support national policies. The national department shares its roles with the provincial education departments for basic education and Early Childhood Development. However, the financing and management of schools is the responsibility of each provincial department (Department of Basic Education, 2018). District offices are directly responsible for interfacing with schools through gathering information and diagnosing various problems in schools. The district offices also perform the important function of facilitating and organizing training for the personnel and directly dealing with funding and resolving bottlenecks as well as solving labor relations disputes. The district offices are critical in ensuring that the school principals are always accountable to provincial education departments and to make sure that the accountability lines within the school to the principal and the school governing bodies are maintained.

Council of education ministers consists of ministers of basic education, higher education, and training as well as the nine provincial members of the executive councils for education. Their responsibility is to discuss how to promote the national education policy (South African Market Access, 2020). They also do their best to share information and views on all the different aspects of education in South Africa. Heads of education departments committee comprised of the Director-General of the department of basic education, the deputy director generals of the department and the heads of the provincial department of education. The purpose of the committee is to make sure they facilitate the development of the national education system, share information and views on national education. The department also helps to coordinate administrative actions on issues of mutual interest and advising the department on matters related to the proper functioning of the national education system. The development and management of a sub-framework of qualifications for the general and FETs is the responsibility of Umalusi. This organization also ensures that the quality standards of the general and FETs are maintained. The word Umalusi means “herder” or “shepherd” which in Nguni culture, is the person who is the guardian of the family’s wealth”. The council is also responsible for the certification of the National Senior Certificate in schools, in FETs, it is responsible for the certification of the National Technical Certificate Level N3 and the National Certificate Vocational (NCV) while in adult education centers, it is responsible for the certification of the General Education Training Certificate.

Umalusi makes sure that learners receive credible certificates, and it makes it a point that it develops and evaluates qualifications and curricula to ensure that they are of the expected standard. Umalusi also moderates assessments to ensure that they are fair, valid, and reliable. The organization also accredits providers of education and training and assessment and research to make sure that educational quality. It also verifies the authenticity of certificates. The National education evaluation development unit ensures that there is an effective evaluation of all the educators premised on the extent to which the learner performance improves. The responsibilities include providing the minister with an effective and independent account of the state of schools, like the quality of teaching and learning in all the schools among other important activities. The Education labor relations council serves the public education sector nationally. The major purpose of the council is to maintain labor peace within public education through processes of dispute prevention resolution. The activities undertaken include collective bargaining between the educator unions and the department of basic education as the employer. The education labor relations council also do workshops to raise the level of awareness and understanding of sound labor relations procedures (Department of Basic Education, 2018). South African Council for educators is a professional council responsible for enhancing the status of the teaching profession and promoting the development of educators and their professional conduct. The functions of the South African council of educators are to register educators and to promote the professional development of educators as well as to set, maintain and protect ethical and professional standards. Educator unions and the schools governing bodies are there to promote the interests of the teachers and parents, respectively.

3. Empirical literature review

Literature on cyber incidents in schools is developing worldwide. Venter *et al.* (2019) discovered that smartphones have penetrated the society of South Africa and are being used daily. As a result, Venter *et al.* (2019) believe that it is important for learners in South Africa to have education on how to secure their devices. To implement this, there must be awareness on the use of these technological devices, especially in schools. However, Venter *et al.* (2019) argued that in South

Africa there is no formal curriculum that addresses cyber incidents in schools. It is only at universities level where cyber security is being taught to students who are studying computer courses. As a result, it is only a handful of young people in South Africa who are aware of cyber incidents risks and subsequently take precautions. Venter *et al.* (2019) posit that cyber incident awareness should be taught in schools, as from an early stage.

Venter *et al.* (2019) agree with Kritzinger (2016) who argued that the rate of technological changes across the globe is somewhat vivid. Kritzinger (2016) noticed that the decreasing costs of internet usage and the availability of ICT devices mean that learners can have access to the Internet through their devices. Kritzinger (2016) believes that learners are integrating Information and Communication Technologies (ICTs) in their daily lives for different reasons like socializing, information gathering and education. The most worrying issue is the fact that learners who use these technologies are not well equipped with skills to protect themselves from cyber incidents and cyber threats (Kritzinger, 2016). It is believed that learners are not well equipped with skills that they can use to safeguard themselves from cyber incidents, especially in developing countries like South Africa. Kritzinger (2016) went on to argue that the national school curriculum in South Africa does not have provisions for cyber-safety education and the availability of supporting materials for training ICT educators is lacking. As a result, educators and learners lack the knowledge and skills about cyber safety. Therefore, Kritzinger (2016) believes that it is important for schools in South Africa to come up with the short term and long-term approach towards cyber-safety among the educators and learners until a formal approach towards cyber-safety is implemented and adopted in South African schools.

Just like the arguments put forward by Kritzinger (2016), Gcaza and Von Solms (2017) also stated that internet usage and access is now a basic human right, and as a result, free wireless Internet has been provided in many cities in the country. However, Gcaza and Von Solms (2017) believe that the national effort to connect South African citizens is not in line with the effort applied to cyber safety. As a result, it is important to come up with a detailed plan on how cyber safety can be cultivated as a culture in South Africa. In another study following on some of the arguments presented by Gcaza and Von Solms (2017), Kritzinger (2020) investigated the current maturity levels of cyber safety in South African schools. According to Kritzinger (2020), maturity levels indicate the level of preparedness of schools to assist educators and learners in establishing a cyber safety culture within the school environment. The author used the UK approved measurement tool, the 360safe tool, to measure cyber safety maturity levels of schools within South Africa. Kritzinger (2020) was looking at leadership and policy, infrastructure, education and standards, and inspection through five levels of compliance. Level 1 indicated that cyber safety measures are aspirational and innovative, and that there is full compliance. Level 5 scores indicated that there is little or nothing in place within the school to ensure cyber safety for learners.

The results indicated that all the 24 schools that participated in the study had significantly low levels of cyber safety maturity compliance. The results further indicated that schools in South Africa are beginning to adopt technology as part of their approaches to prepare learners for the future, but cyber safety awareness policies, practices, and procedures within schools are lagging. In another study, Bada *et al.* (2018) noted that there has been an unprecedented rise in cybercrime globally. Bada *et al.* (2018) argued that Africa is a region with the highest rates of cybercrimes and huge financial losses, yet cybersecurity awareness is very low. Agreeing with Bada *et al.* (2018), Scholtz *et al.* (2019) discovered that it is very important to begin from an early age to educate learners about cyber safety and to ensure that they are aware of the cyber risks. However, Scholtz *et al.* (2019) argued that educators in South African schools do not have the right resources, knowledge, and skills to ensure that learners are aware of the cyber risks.

Rahman *et al.* (2020) also argued that even though the Internet has positively influenced the lives of people, there are negative issues that are emerging related to Internet use. Issues related to cyber bullying, pornography, online fraud, and gambling have risen tremendously due to problems related to lack of awareness and self-mechanism among Internet users. Rahman *et al. (*2020) believe that the level of cyber awareness among Internet users, especially young people, is still low or moderate. Rahman *et al. (*2020) agree with Scholtz *et al.* (2019) and Bada *et al.* (2018) in arguing that one of the ways to cultivate knowledge and awareness among Internet users is to educate young people from an early age. It was highlighted that learners need to be educated to operate safely in cyberspace and to protect themselves. Yan *et al.* (2021) stated that learners and their educators are vulnerable to cyber incidents. Yan *et al.* (2021) also stated that the only way for learners and educators to be able to develop rational judgement and strategies to tackle cyber incidents is to be able to identify both risk factors and protective factors associated with cyber incidents.

4. Research methodology

The researcher conducted a systematic search on literature that reported the extent to which role players responded to cyber incidents in schools. The literature was reviewed employing a systematic literature review of online databases. A qualitative approach and purposive sampling to collect data from the learners was used because it had a promise to yield findings that reflect on the learners' experiences and perceptions on cyber incidents (Levitt *et al.* 2018). A total of 85 learners participated in three 3 focus groups that ranged in size; group one had twenty participants, group two had thirty participants and group three had thirty-five participants. Forty-eight percent were male, and fifty-two percent were female. The rationale for selecting learners was based on the view that cyber aggression is a very concerning issue in the school environment (Lea, 2020). All the conversations were recorded and transcribed. The data was then coded using ATLAS.ti. 7, themes emerged, and the frequencies of these themes were noted by the researcher. In an endeavor to ensure the reliability and validity of data, the verbatim transcribed interviews were presented to the respondents to verify and sign off (Vithal and Jansen, 2010). The researcher reviewed all the transcripts from focus group interviews to check for accuracy, ensuring that no obvious mistakes appeared. The ethical guidelines were followed to ensure that the research study was conducted ethically as prescribed by the University of South Africa and the Department of Basic Education.

The idea behind this qualitative research is to purposefully select participants that are best in helping the researcher to understand the cyber aggression phenomenon in South African high schools and how learners can be helped in cyber space (Maree, 2010). The participants for this research were intentionally selected, depending on the needs of the study (De Vos *et al.* 2009). The participants, that is the learners, were selected according to the defining characteristics that made them the holders of the data needed for the study. This purposive sampling is considered to be "information-rich" informants (McMillan and Schumacher, 2001). Participants were selected according to predetermined criteria relevant to the research objectives.

Table 1. Sample selection

Focus groups N	Males n	Females n	Total Number of participants
1	10	10	20
2	13	17	30
3	18	17	35
Total	41	44	85

As highlighted in Table 1, a total of 85 learners participated in three 3 focus groups that ranged in size; group one had twenty participants, group two had thirty participants and group three had thirty-five participants. Forty-eight percent were male, and fifty two percent were female. The next section is giving the findings of the study.

5. Results: Discussion on the responsibilities of role players in addressing cyber incidents

Reporting cyber incidents is crucial because it is a form of active support for victims and a way to reduce cyber incidents (Barlinska *et al.* 2018). Educators are becoming more aware of cyber incidents, but they still do not know how to intervene (Queensland Government, 2018; DeSmet *et al.* 2015). An effective response to cyber incidents requires a joined approach by government departments, school staff members, learners, parents or guardians, and organizations

(Government of Ireland, 2018). A critical review of the existing literature regarding the role players was done and it revealed that role players lacked a consistent response to reported cyber incidents. The reason is that there is a lack of understanding of the responsibilities of role players in addressing cyber incidents. Schools are confronted with issues of cyber incidents among learners, which they do not know how to respond. There is a significant gap in the literature regarding the responsibilities of role players and how role players should intervene during cyber incidents. The literature review is certainly not exhaustive in its attempt to illuminate how the role players should handle cyber incidents. There is still much that is not known about reporting cyber incidents, especially about the efficacy of efforts to intervene. Figure 1 summarizes the role players that will be discussed in the next section.

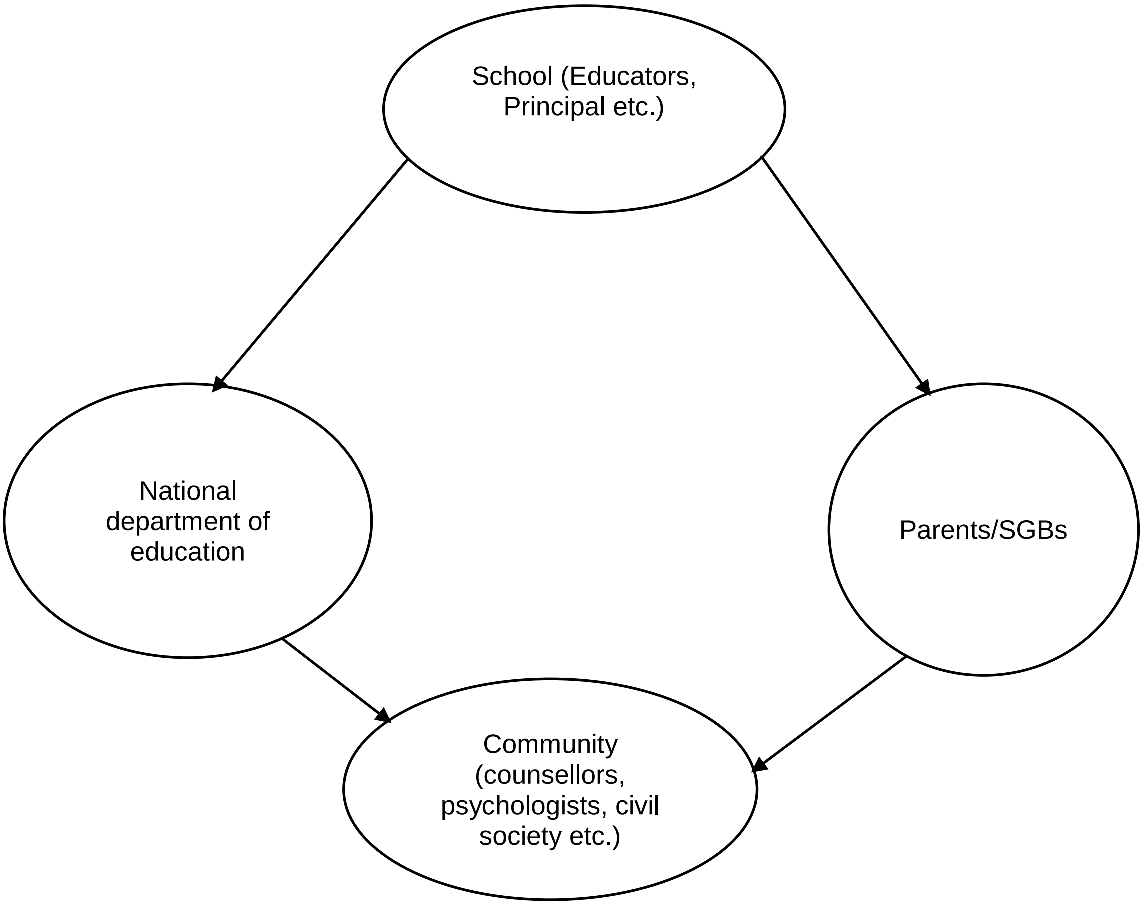
School (Educators, Principal etc.)
National department of education
Parents/SGBs
Community (counsellors, psychologists, civil society etc.)

Figure 1. A summary of role players

In Figure 1, a summary of the role players is given, and these include the school where we have educators, principals, learners and many more. The other classes comprise parents, the community, and the national department of education. A detailed description of the responsibilities of role players is given below. The next section presents some of the recommended role players and the suggested roles and responsibilities in addressing cyber incidents.

5.1. The school/ educators and the principal

The first identified structure is a school, which is supposed to implement procedures that address cyber incidents (Espelage and Hong, 2017). The South African schools should ensure that learners obtain the needed education and knowledge within a cyber incident-free environment (Centre for Justice and Crime Prevention and DBE, 2015). The school staff members have a critical role to play in intervening in cyber incidents among learners. Byrne *et al.* (2016) believe that the school and the staff members should implement cyber incidents intervention and management as part of a systemic whole school approach. It was also stated that to be able to identify cyber incidents, it is important to implement effective management strategies that align with school policies, and to engage in pro-active programs for intervention and bridging the gap between theory and practice. The other important aspect that was highlighted in this research was that it is important to address and reduce cyber incidents by investigating all incidents. Diamanduros, Downs and Jenkins (2008) stated that the school role players like the advisory team, ICT Unit, and the school management board (SMB) need to have roles that are spelt out in the intervention of cyber incidents. Mesch (2009) also outlined that school staff need to be aware of cyber regulatory actions. This can be achieved by coming up with school community capacity building resources, coming up with strategies for responding to cyber incidents and creating effective cyber incidents social environment and policy supports. The other responsibility of the school staff members is to come up with a whole-school online cyber incident intervention and management program (Byrne *et al.* 2016).

Diamanduros *et al.* (2008) argued that the other group with an important role are the school psychologists because they can help in spreading awareness of cyber incidents and the psychological impact on learners. It was also highlighted that school psychologists can play an important role in developing intervention programs that are meant to address the problem of cyber incidents among learners (Diamanduros *et al.* 2008). The other role of school psychologists, as put forward by Diamanduros *et al.* (2008), was that school psychologists are to intervene and plan strategies which schools can implement to reduce cyber incidents. The other role was that psychologists can collaborate with school principals and educators in developing policies that can reduce cyber incidents. Anagnostopoulos *et al.* (2009) also argued that in the United States of America, expansion of efforts to engage school staff in the intervention process is one of the effective ways of reducing cyber incidents. Leoschut and Kafaar (2017) added that it is also important for school educators and all the role players to understand the forms of victimization which the learners are experiencing in order to come up with critical interventions in assisting learners. Kritzinger (2016) stated that school learners are not educated enough on the techniques of using technological devices safely, particularly in developing countries like South Africa. Since the school curriculum in South Africa does not have the provisions for cyber safety education the school needs to create an environment that will allow learners to know more about the negative effects of cyber incidents.

5.2. The parents/ school governing board (SGB)

Parents should be involved in monitoring the online behaviors of their children and they should communicate with their children about online challenges. According to Cross *et al.* (2015), this can be achieved by developing appropriate online support for learners and building a good relationship between learners and parents. The researchers also highlighted that agreements about learners' online behavior and online skill-building should be put in place. Parents should address cyber aggression to determine how best to intervene. This can be achieved by setting up appropriate limits on screen time, monitoring their children's use of technology, talk to their children about internet safety and privacy, and identifying why their children are not talking to them about their online experiences (Espelage and Hong, 2017). These parents' responsibilities were supported by various scholars like Helfrich *et al.* (2020), Makri-Botsari and Karagianni (2014) and Mesch (2009), among others. Mesch (2009) argued that cyber incidents are experienced more by learners who are active on social media, with active profiles on various network sites and those who participate in chat rooms. The author also indicated that parental mediation techniques can help to protect learners from cyber risks. Finally, the author highlighted that it is important to have more parental participation to reduce risks of cyber incidents that arise from cyber space.

Makri-Botsari and Karagianni (2014) discovered that though parenting styles are not significant in predicting learners' cyber victimization, it was a strong predictor of cyber incident manifestation. It was found that adolescents with authoritative parents showed the lowest levels of cyber threatening behaviors. Makri-Botsari and Karagianni (2014) also discovered that learners with authoritative parents communicated more frequently with them on their cyber incident experiences compared to learners with permissive and neglectful parents. Helfrich *et al.* (2020) also researched on the role of parents in the intervention during cyber incidents among learners since some of the problems of cyber incidents happen at home. Helfrich *et al.* (2020) discovered that it is important to have effective communication between parents and their children on issues related to cyber incidents. The study by Helfrich *et al.* (2020) also found that monitoring and the availability of professional resources are key issues that need to be taken seriously by parents in dealing with cyber incidents. The parent should make sure that internet ethics are cultivated in their children; parents should be more intensively in supervising the development of their children against the influence of cyber incidents.

5.3. The national department of education

The department of basic education has a responsibility to create an environment that creates solutions for cyber incidents in schools. Cassidy *et al.* (2013) believe that the department of basic education should partner with schools in finding appropriate solutions to cyber incidents among learners since there is a strong interrelationship between negative online interactions at school and cyber incidents through home computers and cell phones. The DBE together with the industry should adequately resource and support schools in implementing cyber safety strategies (Kritzinger, 2020). The department should formulate policies that will assist educators and learners when they are reporting cyber incidents, it should also foster an environment for collaboration between role players, monitor and evaluate the cyber incident policies for schools and make sure that these schools have cyber incidents policies. The department should also make sure that resources and support are available for learners and that the school board of management is helping the school (Government of Ireland, 2018). Childnet International (2016) also pointed out that the welfare of learners should be taken as a responsibility of everyone, but Kritzinger (2020) pointed out that the Department of Basic Education should make sure that it creates an environment that all stakeholders see to it that it is their responsibility to ensure that learners are cyber secure. Sakban *et al.* (2018) also pointed out that it is the responsibility of the national department of education to undertake regularly updated learner protection training, which includes understanding the intervention processes and how to respond to cyber incidents.

Sakban *et al.* (2018) pointed out that the police can play a critical role in preventing cyber incidents, but it is the responsibility of the national department of education to see to it that an environment is created for the police to be able to intervene. Sakban *et al.* (2018) pointed out that the police can help to reduce cyber incidents through fostering socialization with educational institutions and society regularly. The police can conduct routine anti-cyber incidents campaigns in schools, institutions, and in communities and involve social organizations in monitoring cyber incidents. However, Sakban *et al.* (2018) pointed out that the actions of the police in preventing cyber incidents cannot manifest as a stand-alone but there must be cooperation with the various stakeholders like the national department of education, the provincial department, the district department, and the school. International Telecommunication Union (2009) pointed out that the national government is a critical stakeholder in leading national cyber safety efforts that can assist all involved stakeholders. It was highlighted that apart from putting measures to counter cyber incidents, national governments have the central role to establish among the stakeholders the awareness and understanding of cyber incidents as a responsibility for all stakeholders. International Telecommunication Union (2009) also pointed out that it is the responsibility of the national government in partnership with the various departments of education to come up with a national cyber safety strategy that can help to provide a common understanding and vision of the problem among all the stakeholders. In different countries, the national cyber safety strategies are mostly formulated at the high level of government, spearheaded by the head of government to ensure that there is a buy-in of all the stakeholders. One example is Brazil where the cyber safety and cyber security strategies are led by the office of the President in partnership with the various stakeholders such as the department of education, the police and community organizations including civil society (Redmond *et al.* 2020).

5.4. The community and the civil society

The last structure is the community, with role players such as counsellors, psychologists, Children's Rights Centers, Internet Service Providers, phone companies, attorneys, media, and the police. Educational efforts by Social Media Service Providers (SMSP) could enhance the anti-cyber aggression efforts for schools and parents. The police have an important role to play in supporting schools in achieving and maintaining cyber safety (Centre for Justice and Crime Prevention and DBE, 2015). The attorneys can be of assistance in terms of pending civil action that could be taken against the aggressors (Redmond *et al.* 2020; Cellphone Safety, 2011). Sometimes more serious or repeat cyber incidents might need to involve role players outside the school who can provide specific and specialized interventions and support. The interests of the community in various nations are represented by civil society groups who take the various form of functions. Some of the groups include consumer rights advocacy organizations and environmental groups.

In countries such as the United States of America and Canada, civil society groups are increasingly taking a greater interest in cyber safety as they appreciate the various issues that the community such as human rights, civil liberties, privacy, and consumer protection among many are undertaking. Civil society groups take part in various consultations with the government to provide feedback and other contributions which act as a source of information for policymaking that helps to create a holistic cyber safety strategy (Scholtz *et al.* 2020). The civil society in partnership with various role-players also helps to provide the awareness on how the learners can manage cyber risks adequately (Topcu and Erdur-Baker, 2012). It is argued that capacity building is a critical complement in building cyber incident awareness and for the culture of cyber safety to be established and cyber safety competency to be increased. This can be achieved by increasing the trainings related to cyber safety. The literature review was also conducted to identify the responsibilities of role players to address cyber incidents. While it may take a village to raise a child, the virtual village inclusive of social media platforms, Internet Service Providers, phone companies, non-profit youth organizations, non-governmental organizations, educational institutions, parents or guardians, attorneys, and media, need to join forces to nationally and globally dialogue on ways to protect learners from cyber incidents (Tinstman Jones *et al.* 2020).

6. The needs of role players

From the reviewed literature, the needs for role players were identified so as to outline role players' responsibilities when responding to cyber incidents. Role players should be informed of cyber incident reporting procedures, role players should know what to do when they become aware of or suspect any cyber incident taking place, and role players need a referral system, and community partnerships to support learners. Table 2 summarizes the identified needs and the respective role players. The aim is to ensure relevant role players are drawn in to create a supportive structure that can contribute to addressing cyber incidents in South African schools.

Table 2. Needs for role players and a summary of their responsibilities

Needs for Role Players	Role Players and Responsibilities
Outline responsibilities for role players when responding to cyber incidents.	• The principal should ensure that school personnel and parents can address cyber incidents. • The advisory Team should implement an effective approach in intervening and responding to all cyber incidents. • Educators should be aware of the steps to take and advice to give if learners notify them of cyber incidents. • Parents should report their children's cyber aggression.
All role players should be informed of the cyber incident reporting procedures. *The school community should know what to do when they become aware of or suspect any cyber incident taking place.*	• The advisory team should establish a process that communicates the cyber incident reporting procedures to all parents, learners, and all staff members. • The School Management Board (SMB), School Governing Bodies (SGB) and Counsellors should explain the cyber incident reporting procedures to learners and their parents or guardians. • Social Media Service Providers should improve the visibility, consistency, and accessibility of reporting tools on their platforms.
Need a referral system for services and community partnerships to support learners and build a cyber school safe environment.	• The South African Police Service (SAPS) should be obliged to investigate any unlawful cyber incidents in schools. • Learners should contact SAPS in case of any cyber incident. • Counsellors should give immediate support to all affected learners. • Parents should partner with schools to ensure that their children are following appropriate guidelines for online behavior. • Parents of the victims should be able to work with the Internet Service Provider, Cell Phone Service Provider, or Content Provider to investigate the cyber incident. • Internet Service Providers should track instant messaging which could be used as evidence in a court of law. • The Child Protection and Abuse Organization should be contacted for help if a cyber incident is a suspected child protection issue. • SA Depression and Anxiety Group (SADAG) should assist learners suffering emotionally because of the cyber incident ordeal. • Educational Organizations should continue to hold workshops, do research, and give presentations on cyber safety topics to help the school communities. • The attorneys should be able to provide parents with sound legal advice on how to open possible criminal cases and how to get restraining orders against the accused.

Source: Author's analysis

7. Learners' perceptions about adults on issues of cyber incidents

The results from the focus group interviews have shown that learners are acutely aware of cyber incidents occurring in their schools, but they are reluctant to report their experiences of cyber incidents. If cyber incidents are left unaddressed, they can have a devastating effect on learners; they can create a barrier to learning and have serious consequences on the mental wellbeing (Chen, 2020). Learners believe that adults are unsure on how to deal with cyber incidents; adults do not know about the most effective interventions strategies to use to address cyber incidents. Learners also indicated that adults' interventions are ineffective and are not yielding any positive results, adults do not know their roles in the intervention during cyber incidents, and there is nothing or little adults can do to intervene during cyber incidents. Learners believe that adults are called upon to solve cyber incidents that transcend over their level of expertise and capacity, and with law enforcement, it is not known how cyber incidents are solved or what the outcomes are. According to learners, reporting is useless and counterproductive, school management's response is ineffective or aggravates the problem and nothing is done by the school management board. Learners do not have an idea how schools handle cyber incidents and what consequences are for the aggressors and adults cannot intervene or provide consequences. From the perception of learners on adults, they do not have confidence in adults. From the interviews, the two conflicting ideas emerged are: There is little or nothing adults can do and most of their attempts to intervene are ineffective, and Adults need to assist learners in handling cyber incidents. This then means that adults must educate themselves to be able to assist learners in addressing cyber incidents.

8. Conclusion

As ICT use is likely to increase and be relevant to learners, especially with online teaching and learning during and post Covid-19, cyber aggression will also continue to be an issue in schools worldwide. Learners are largely unaware of these risks; and so, they put themselves at risk. In recognition of this, the study concludes that better access to information about where, how and to whom can learners report cyber incidents is needed. Therefore, the study aimed to outline the responsibilities of role players and how role players should assist in responding to cyber incidents. The aim is to ensure that all relevant role players are drawn in to create a supportive environment for proper handling of cyber incidents in schools. The literature reviewed and the focus group interviews resulted in the development of the roles and responsibilities of the various role-players. The researcher recommends that these responsibilities be communicated and become readily available to learners, parents or guardians and all involved role players. What is evident from the research is that many role players can or need to be involved in handling cyber incidents in schools. The study also discovered that role players cannot work in isolation, rather, they need a coordinated approach to share the responsibilities as cyber incidents are not restricted to the classroom or school grounds. This problem requires all role players to work together, in proactive ways to intervene and reduce cyber incidents. It emerged from this study that some areas or topics require more research. Qualitative research is needed to provide opportunities to the cyber incident aggressors to highlight their perceptions and experiences. Research into the role of bystanders needs to be addressed. Lastly, how learners are using technology to hide information from parents can be another area of research.

References

Anagnostopoulos, D., Buchanan, N. T., Pereira, C., and Lichty, L. F., 2009. School staff responses to gender-based bullying as moral interpretation: an exploratory study. *Educational Policy*, 23(4), pp. 519–553. https://doi.org/10.1177/0895904807312469

Angus, C., 2016. *Cyberbullying of children: E-Brief.* Australia.

Astatke, M., Weng, C. and Chen, S., 2021. A literature review of the effects of social networking sites on secondary school students' academic achievement. *Interactive learning Environments,* (2021), pp. 1–17. https://doi.org/10.1080/10494820.2021.1875002

Bada, M., Von Solms, B. and Agrafiotis, I., 2018. *Reviewing national cybersecurity awareness in Africa: An empirical study.* Thinkmind Digital Library, 2018.

Barlinska, J., Szuster, A. and Winiewski, M., 2018. Cyberbullying among adolescent bystanders: Role of affective versus cognitive empathy in increasing prosocial cyberbystander behavior. *Frontiers in Psychology,* 9(2018), p. 799. https://doi.org/10.3389/fpsyg.2018.00799

Bulger, M., Burton, P., O'Neill, B. and Staksrud, E., 2017. *Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online, new media & society.* [PDF] Available at:

<http://www.cjcp.org.za/uploads/2/7/8/4/27845461/protecting_children_online.pdf> [Accessed on 3 March 2018.

Burton, P., Leoschut, L. and Phyfer, J., 2016a. *South African kids online: A glimpse into children's internet use and online activities, Cape Town.* [PDF] Available at: <http://www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf> [Accessed on 17 November 2017].

Burton, P., Leoschut, L. and Phyfer, J., 2016b. *South African kids online: barriers, opportunities, and risks. A glimpse into South African children's internet use and online activities*. Techical Report. Cape Town.

Byrne, J., Kardefelt-Winther, D., Livingstone, S. and Stoilova, M., 2016. Global kids online research synthesis, 2015-2016. London.

Cassidy, W., Faucher, C. and Jackson, M., 2013. Cyber bullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. *School Psychology International,* 34(6), pp. 575–612. https://doi.org/10.1177/0143034313479697

Cellphone Safety, 2011. *Cyber bullying 3 of 3: When all else fails.* [online] Available at: <http://www.cellphonesafety.co.za/cyber-bullying-3-of-3-when-all-else-fails.html> [Accessed on 23 February 2014].

Centre for Justice and Crime Prevention and DBE, 2015. *The national school safety framework.* Cape Town.

Chen, J. K., 2020. Cyber victimisation, social support, and psychological distress among junior high school students in Taiwan and Mainland China. *Asia Pacific Journal of Social Work and Development,* 30(3), pp. 150–163. https://doi.org/10.1080/02185385.2020.1755994

Childnet International, 2016. *Cyberbullying: Understand, prevent, and respond - Guidance for schools*. London.

Cilliers, L. and Chinyamurindi, W., 2020. Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa. *Electronic Journal of Information Systems in Developing Countries (EJISDC),* 86(4), pp. 1–10. https://doi.org/10.1002/isd2.12131

Cross, D., Barnes, A., Papageorgiou, A., Hadwen, K., Hearn, L. and Lester, L., 2015. A social-ecological framework for understanding and reducing cyberbullying behaviours. *Aggression and Violent Behavior,* 23(2015), pp. 109–117. https://doi.org/10.1016/j.avb.2015.05.016

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., Thomas, L. and Barnes, A., 2016. Longitudinal impact of the cyber friendly schools program on adolescents' cyberbullying behavior. *Aggressive Behaviour,* 42(2), pp. 166–180. https://doi.org/10.1002/ab.21609

Department of Basic Education, 2017. *Guidelines on e-Safety in Schools: Educating towards responsible, accountable and ethical use of ICT in Education.* Pretoria.

Department of Basic Education, 2018. *Education statistics in South Africa 2016.* Department of Basic Education.

DeSmet, A., Aelterman, N., Bastiaensens, S., Van Cleemput, K., Poels, K., Vandebosch, H., Cardon, G. and De Bourdeaudhuij, I., 2015. Secondary school educators' perceptions and practices in handling cyberbullying among adolescents: a cluster analysis. *Computers and Education,* 88(2015), pp. 192–201. https://doi.org/10.1016/j.compedu.2015.05.006

Diamanduros, T., Downs, E. and Jenkins, S. J., 2008. The role of school psychologists in the assessment, prevention, and intervention of cyberbullying. *Psychology in the Schools,* 45(8), pp. 693–704. https://doi.org/10.1002/pits.20335

Espelage, D. L. and Hong, J. S., 2017. Cyberbullying prevention and intervention efforts: Current knowledge and future directions. *The Canadian Journal of Psychiatry,* 62(6), pp. 374–380. https://doi.org/10.1177/0706743716684793

Farhangpour, P., Maluleke, C. and Mutshaeni, H. N., 2019. Emotional and academic effects of cyberbullying on students in a rural high school in the Limpopo province, South Africa.

South African Journal of Information Management, 21(1), pp. 1–8. https://doi.org/10.4102/sajim.v21i1.925

Gcaza, N. and Von Solms, R., 2017. A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries,* 80(1), pp. 1–17. https://doi.org/10.1002/j.1681-4835.2017.tb00590.x

Government of Ireland, 2018. *Action plan for online safety - 2018/2019 - Ireland, action plan.* [online] Available at: <https://assets.gov.ie/162/120718132737-7082532-ONLINE SAFETY ACTION PLAN 2018-2019.pdf> [Accessed on 1 September 2019].

Helfrich, E. L., Doty, J. L., Su, Y. W., Yourell, J. L. and Gabrielli, J., 2020. Parental views on preventing and minimizing negative effects of cyberbullying. *Children and Youth Services Review,* 118(2020), p. 105377. https://doi.org/10.1016/j.childyouth.2020.105377

Hellsten, L. M., 2017. *An introduction to cyberbullying*. Macerata.

Hills, C. A., 2017*. Developing a law and policy framework to regulate cyber bullying in South African schools.* University of South Africa.

International Telecommunication Union, 2009. Cybersecurity: The role and responsibilities of an effective regulator. In: 9th ITU Global Symposium for Regulators. Beirut, Lebanon, p. 16.

Kowalski, R. ., Limber, S. P. and McCord, A., 2019. A developmental approach to cyberbullying: Prevalence and protective factors. *Aggression and Violent Behavior*, 45(2019), pp. 20–32. https://doi.org/10.1016/j.avb.2018.02.009

Kritzinger, E., 2016. Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, 28(1), pp. 1–17. https://doi.org/10.18489/sacj.v28i1.369

Kritzinger, E., 2020. Improving cybersafety maturity of South African schools. *Information*, 11(10), pp. 471–488. https://doi.org/10.3390/info11100471

Lea, Q. T., 2020. A study of the core relationship between cyber-bullying and coping of high-school pupils in Vietnam. *International Journal of Innovation, Creativity and Change*, 11(3), pp. 483–500.

Leoschut, L. and Kafaar, Z., 2017. The frequency and predictors of poly-victimisation of South African children and the role of schools in its prevention. *Psychology, Health & Medicine*, 22(1), pp. 81–93. https://doi.org/10.1080/13548506.2016.1273533

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R. and Suárez-Orozco, C. 2018. Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force report. *American Psychologist,* 73(1), pp. 26–46. https://doi.org/10.1037/amp0000151

Makri-Botsari, E. and Karagianni, G., 2014. Cyberbullying in Greek adolescents: The role of parents. *Procedia - Social and Behavioral Sciences,* 116(2014), pp. 3241–3253. https://doi.org/10.1016/j.sbspro.2014.01.742

Maree, K., 2010. *First steps in research.* Van Schailk.

Martin, F., Wang, C., Petty, T., Wang, W. and Wilkins, P., 2018. Middle school students' social media use. *Educational Technology & Society,* 21(1), pp. 213–224.

McCoy, S. and Lyons, S., 2018. *Digital technologies and student learning*. Ireland's yearbook of education 2018-2019. Education Matters.

McMillan, J. H. and Schumacher, S., 2001. *Research in education: A conceptual Introduction.* Boston: Longman.

Meier, E. B., 2021. Designing and using digital platforms for 21st century learning. *Educational Technology Research and Development*, 2021(1), pp. 1–4. https://doi.org/10.1007/s11423-020-09880-4

Mesch, G. S., 2009. Parental mediation, online activities, and cyberbullying. *CyberPsychology & Behavior*, 12(4), pp. 387–393. https://doi.org/10.1089/cpb.2009.0068

Mhlanga, D., 2020. Industry 4.0: The challenges associated with the digital transformation of education in South Africa. *International Journal of Financial Studies,* 8(3), pp. 45. https://doi.org/10.3390/ijfs8030045

Mhlanga, D. and Moloi, T., 2020. COVID-19 and the digital transformation of education: What are we learning on 4IR in South Africa? *Education Sciences,* 10(7), p. 180. https://doi.org/10.3390/educsci10070180

Myers, C. A. and Cowie, H., 2019. Cyberbullying across the Lifespan of Education: Issues and Interventions from School to University. *International Journal of Environmental Research and Public Health*, 16(7), pp. 1–14. https://doi.org/10.3390/ijerph16071217

Phyfer, J., Burton, P. and Leoschut, L., 2017. *South African kids online*. Cape Town.

Queensland Government, 2018. *Adjust our settings: A community approach to address cyberbullying among children and young people in Queensland*. Queensland.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M. and Khalid, F., 2020. The importance of cybersecurity education in school. *International Journal of Information and Education Technology,* 10(5), pp. 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Redmond, P., Lock, J. V. and Smart, V., 2020. Developing a cyberbullying conceptual framework for educators. *Technology in Society*, 60(2020), p. 101223. https://doi.org/10.1016/j.techsoc.2019.101223

Sakban, A., Sahrul, S., Kasmawati, A. and Tahir, H., 2018. The role of police to reduce and prevent cyber-bullying crimes in Indonesia. *Advances in Social Science, Education and Humanities Research*, 192(2018), pp. 36–41. https://doi.org/10.2991/icils-18.2018.7

Scholtz, D., Kritzinger, E. and Botha, A., 2019. Underpinning Knowledge and Skills for Educators to Enhance Cyber Safety Awareness in South African Schools. In: International Conference on Innovative Technologies and Learning. Cham: Springer. pp. 278–290. https://doi.org/10.1007/978-3-030-35343-8_30

Scholtz, D., Kritzinger, E. and Botha, A., 2020. Cyber safety awareness framework for South African schools to enhance cyber safety awareness. In: Computer Science Online Conference. Cham: Springer, pp. 216–223. https://doi.org/10.1007/978-3-030-51974-2_19

South African Market Access, 2020. *Education statistics - South African market insights.* [online] Available at: <https://www.southafricanmi.com/education-statistics.html> [Accessed on 2 August 2021].

Tinstman Jones, J. L., Campbell, L. O., Stickl Haugen, J. and Sutter, C. C., 2020. Cyberbullying considerations for school counselors: A social media content analysis. *Professional School Counseling*, 23(1). https://doi.org/10.1177/2156759X20919365

Topcu, C. and Erdur-Baker, O., 2012. Affective and cognitive empathy as mediators of gender differences in cyber and traditional bullying. *School Psychology International,* 33(5), pp. 550–561. https://doi.org/10.1177/0143034312446882

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), p. e02855. https://doi.org/10.1016/j.heliyon.2019.e02855

Vithal, R. and Jansen, J. D., 2010. *Designing your first research proposal: A manual for researchers in education and the social sciences*. Juta.

De Vos, A. S., Strydom, H. and Fouche, C. B., 2009. *Research at grassroots for the social sciences and human service professions*. Pretoria: Van Schaiks.

Yan, Z., Xue, Y. and Lou, Y., 2021. Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, 121(2021), p. 106791. https://doi.org/10.1016/j.chb.2021.106791