Cyber Incident Handling Framework for Schools in South Africa: Views of Experts

Naume Sonhera
Vaal University of Technology

The goal of this study was to create a Cyber Incident Handling Framework (CIHF) for South African schools to improve their effectiveness in dealing with cyber incidents while also ensuring that each role player plays an important role in the intervention process aimed at reducing cyber incidents in schools. Experts' comments on the proposed cyber incident handling framework (CIHF) for schools in South Africa were gathered through an expert review survey. The use of expert reviewers was justified to tap into the reviewers' expertise and knowledge. The expert opinion was useful in determining the relevance of the suggested framework, reflecting on its quality, and determining how well it supports the solution of reporting cyber events in South African schools. The expert review process' significant contribution was the documentation of expert opinions on the planned CIHF for South African schools. The study detailed the Cyber Incident Handling Framework (CIHF), as well as the problems in applying the framework and how the challenges may be handled.

Keywords: cyber, incident, experts, survey, expert reviewers, learner, school, report, South Africa, role player, framework

INTRODUCTION

New information and communication technologies (ICTs) and the vast proliferation of social media platforms have become an integral part of everyday life and have greatly influenced interpersonal communication and engagement worldwide. Learners represent the largest and fastest-growing group of users of the internet and they have grown up immersed in technology from a young age (Goodyear, 2020). As learners increasingly engage in technology, there is a heightened concern for their safety online. Sonhera et al., (2020) acclaimed that when it comes to dealing with cyber incidents in South African schools, the main difficulty is that there are no clear duties and responsibilities for essential role-players. Learners are vulnerable in cyberspace and require adult and peer protection, assistance, and support from preschool to university, learners a generation that has grown up with technology (Sonhera et al., 2020 Mhlanga Moloi2020). Sonhera (2020) also claimed that technology has become a right for all learners, which explains why it is used widely throughout their daily lives, far outnumbering how it is used by adults. The usage of ICTs in South African schools is also increasing, according to the Department of Basic Education (2017). Learners are invited to browse websites at their leisure to see course materials. While learners in South African schools are becoming more aware of the internet, Kritzinger (2020) claims that they are not becoming more conscious of safe procedures when using ICTs. As they strive for technology literacy, learners receive inconsistent messages about online behaviour, sometimes without the assistance they need.

Learners appear to be uninformed of the dangers of inappropriate online behavior, dismissing them as minor. Learners in South Africa are not immune to cyber incidents.

According to Richardson et al., (2020), cybersecurity has emerged as one of the most pressing concerns affecting schools in the twenty-first century, and computer security is a key tool for safeguarding children. Richardson et al., (2020) went on to say that K 12 schools are one of the most appealing targets for data privacy crimes, owing to schools' ineffective cybersecurity policies. The human component was cited as one of the reasons for the success of many assaults on school computers and systems, as the untrained computer user is the weakest link targeted by cyber thieves using social engineering. To prevent computer hackers and attackers from exploiting human vulnerabilities, Richardson et al., (2020), feel that formal cyber security knowledge is essential. Pencheva et al. (2020) examined the drivers and challenges to incorporating cybersecurity into the high school curriculum and found that learners, while more aware of cyber incidents than their teachers, lacked comprehension of online safety and educators lacked sufficient information and resources.

Schools, just like other institutions, are vulnerable to cyber-attacks, according to Goran (2017). And this vulnerability has been highlighted in recent years, as the number of attacks against public schools has increased and taken on increasingly diverse forms. According to Goran (2017), today, learners' grades, disciplinary notes, learning diagnoses, phone numbers, addresses, and other identifying information are all at risk of being disclosed. The fact that poor network security poses a grave threat to parents of schoolchildren whose personal records contain sensitive or hazardous information is another important issue. As a result, Goran (2017) argues that the practical consequences of these attacks necessitate intervention or remediation to improve cyber security. In addition, when storage facilities or compromised devices are put into systems, cyber-attacks may occur. Again, operators' careless or malicious actions expose or change sensitive information regarding learners' mental and emotional health, future postgraduate plans, and social security numbers (Goran 2017 Mhlanga 2020, Mhlanga 2021).

Existing evidence suggests that in South Africa, there is a paucity of laid-down procedures that are consistently followed by schools to address cyber incidents (Cilliers and Chinyamurindi, 2020, Bulger, Burton, O'Neill and Staksrud, 2017). This paucity impacts negatively transparency, appropriateness, and consistency of investigation and response mechanisms in the event of cyber incidents (Hills, 2017; Burton, Leoschut, and Phyfer, 2016). The purpose of the current study was to develop a Cyber Incident Handling Framework (CIHF) for schools in South Africa to enhance the effectiveness in handling cyber incidents as well as ensure each role player has an important contribution in the intervention process that is designed to reduce cyber incidents in schools. The proposed overall Cyber Incident Handling Framework was presented to the expert reviewers as a collation of individual components or processes.

PURPOSE OF THE RESEARCH STUDY

This research study is proposing CIHF for South African schools. In this research paper, expert opinion helped to determine the relevance of the proposed framework, to reflect on the quality of the framework, and the extent to which the framework supports the solution of reporting cyber incidents in South African schools (Peffers, Tuunanen, Rothenberger and Chatterjee, 2007). An expert can be defined as a person who has specific, valuable skills and exceptional knowledge in a specific area of specialty (Maclellan and Soden, 2003). An expert can also be defined as someone who can think effectively and strategically about a problem because of their vast amount of knowledge in a specialized area (Chi, Glaser and Farr, 2014). This research paper did not seek a new definition for the term "expert", it merely adopted the definitions provided by Chi, Glaser and Farr (2014), and by Maclellan and Soden (2003). i.e., experts are people with very specific valuable skills and exceptional knowledge in an area of specialty and are highly specialized, to the extent that they can make sound decisions about a problem and critically evaluate information. Data was collected from the expert reviewers in the form of feedback from experts on the CIHF.

FRAMEWORKS, PROCEDURES, AND GUIDELINES FOR DEALING WITH ONLINE ISSUES

According to Cichonski et al. (2012), an incident response framework is a plan that provides a conceptual foundation to enable incident response operations. The aspects of the mission, services, people, process, technology, and facilities are all included in a plan. Cyber incident handling, or incident response, on the other hand, is a structured strategy for dealing with and managing the aftermath of a security breach or cyber incident, computer incident, or security event.

The goal is to manage the situation in such a way that harm is limited, and recovery time and expenditures are minimized. The UK Council for Child Internet Safety (UKCCIS) was established to help learners to be safe online (Gov.UK, 2017). The UKCCIS education group produced guidelines for school governors, governing boards, and school leaders to assist learners to be safe online (Gov.UK, 2017). In Germany, an awareness campaign called “klicksafe” was introduced to promote media literacy and adequate handling of the internet and media (EU, 2017). The objective of klicksafe is to make the public more aware of the importance of safe internet use for learners. The research done by a task force for the Queensland government (2018) recommended public education campaigns about cyber incidents, particularly on how to prevent cyber incidents in schools, where to obtain help, and how to report them. The task force indicated that campaigns should be aimed at parents, guardians, school staff members, and learners, with a particular emphasis on changing bystander behaviour to that of upstanders. A report on a community approach to addressing cyberbullying among children and young people was produced. The framework provides guidance and standards on how cyber incidents can be addressed (Queensland Government, 2018).

In 2015 the, Centre for Justice and Crime Prevention (CJCP), in collaboration with the then-national Department of Education (now the DBE), introduced the National School Safety Framework (NSSF). The framework provides the minimum standards for safety in South African schools that should be established, implemented, and monitored, and for which schools, districts, and provinces can be held accountable (CJCP and DBE, 2015). The framework addresses some of the main types of violence that occur in schools, or that relate to the school experience, i.e., physical bullying; xenophobia; homophobia; corporal punishment; sexual and gender-based violence; assault and fighting; and gang violence. The document addresses violence in general, mainly physical violence. Suggestions from these frameworks, guidelines, and procedures were adopted by the researcher and were used as the basis for developing a CIHF for South African schools.

EMPIRICAL LITERATURE REVIEW

Information technology (IT) curricula now include computer security incident response as a key component. Because the incident response is such a difficult task, developing a successful incident response capability necessitates a lot of planning and resources (Cichonski et al.,2012)

Rahman et al., (2020) believe that even though the internet has had a good impact on people's lives, there have been some negative consequences associated with its use. Due to a lack of awareness and self-mechanism among internet users to protect themselves from becoming victims of cyberbullying, online fraud, racial abuse, pornography, and gambling, cases of cyber-bully, online fraud, racial abuse, pornography, and gambling have increased dramatically. Rahman et al., (2020) also believe that past research revealed that the level of awareness among internet users is still low or moderate and one of the vital measures to be taken is to cultivate knowledge and awareness among internet users from their early age, like young children. Rahman et al., (2020) also believe that young children specifically, need to be educated to operate safely in cyberspace and to protect themselves in the process.

In South Africa, Cilliers and Chinyamurindi (2020) researched student teachers' opinions of cyberbullying in elementary and high schools. According to Cilliers and Chinyamurindi (2020), cyberbullying has become a hot topic among South African learners. The South African Department of Basic Education, on the other hand, provides virtually little guidance for schools on how to deal with cyberbullying. The results of a qualitative poll showed that cyberbullying is a severe issue in schools, but that the concept has yet to be incorporated into policy or the school curriculum. According to Cilliers and Chinyamurindi (2020), the South African Department of Basic Education should develop a uniform policy that schools may utilize to adopt and enforce cyber safety in the classroom.

Kortjan and Von Solms (2013) also said that the internet is becoming more integrated into the daily lives of many people, organizations, and countries. Kortjan and Von Solms (2013) also claimed that the internet has had a favourable impact on how individuals communicate to a great extent. It has also opened new economic opportunities and provided governments with the ability to govern online. The other argument is that, while cyberspace provides an unlimited list of services and opportunities, it also comes with many threats, one of which is cybercrime, and the internet has provided criminals with a platform on which to flourish and expand. Kortjan and Von Solms (2013) went on to say that because of the abstract nature of the internet, it is easy for criminals to go unpunished, and many internet users are unaware of such risks; as a result, they, as well as businesses and government assets and infrastructure, may be at risk.

As a result, cyber security awareness and education activities are required to promote users who are not knowledgeable about the risks linked with the internet.

According to Kritzinger (2016), the rate of technological advancement around the globe is rapid, and the dropping cost and rising availability of ICT equipment imply that their users are no longer limited to industrial or government professionals but are now also at home. Home users, according to Kritzinger (2016), use ICT in their daily life for education, socializing, and information gathering. Kritzinger (2016), like Kortjan and Von Solms (2013), believes that utilizing ICT is linked to hazards and threats including identity theft and phishing scams. Most home users of ICT, according to Kritzinger (2016), lack the requisite information technology and internet abilities to secure themselves and their information. Schoolchildren, particularly in impoverished nations like South Africa, are not fully instructed on how to use modern equipment responsibly. Again, according to Kritzinger (2016), the national school curriculum in South Africa does not currently include cyber-safety instruction, and the availability of supporting material and training for ICT educators are restricted, resulting in a lack of cyber-safety knowledge and abilities.

Kritzinger (2017) noted in another study that practically all school learners now have access to ICT gadgets and the internet at home or at school. Kritzinger (2017) went on to say that more and more schools in South Africa are using ICT devices to boost education. ICT equipment and internet connectivity have numerous benefits that help learners learn more effectively and educators teach more effectively. Again, according to Kritzinger (2017), these benefits come with a slew of ICT and cyber-risks and hazards that can affect learners, such as cyberbullying, identity theft, and access to unsuitable information. South Africa now lacks a long-term strategy for instilling a cyber-safety culture in its educational institutions. Kritzinger (2017) even proposed a short-term initiative in the shape of a game-based method to help learners become more cyber-safe and teach them about the important cyber-related hazards and threats.

Sonhera et al., (2021) also researched to assess role actors' duties in dealing with cyber events in South African schools. Cyber events, according to Sonhera et al., (2021), are posing significant issues for school officials worldwide who are called upon to respond to these incidents involving learners. Online threats, according to Sonhera et al., (2021), fly under the radar of educators and parents, making it difficult to address cyber incidents in schools and even more difficult to monitor off-campus activities. One of the most significant challenges in South African schools is that there are no clear roles and responsibilities for relevant role-players when dealing with cyber incidents. The duties of numerous role-players, including the school with its educators, principal and learners, the Department of Basic Education, the community, and the parents, were documented by Sonhera et al., (2021). The study concluded that cyber incidents in schools can be decreased if role players take their duties and responsibilities seriously.

Hettema (2021) created a paradigm for using rationality constraints in cyber event response, attribution, and threat intelligence. Handling, analysis, and attribution, according to Hattema (2021), require 'epistemic states,' which are based on a limited grasp of the attackers' intentions, opportunities, actions, and specific motions. One of the most critical duties in cyber security incident handling, according to Lif et al., (2018), is to report what has happened. Several frameworks have been developed to assist this reporting, according to Lif et al., (2018), each with its own set of benefits and drawbacks.

A set out to determine the acceptability of sixteen plausible information items linked to traceability and analysis as a first step in the construction of a practically effective event description standard was done, according to Lif et al., (2018). The findings of Lif et al., (2018) reveal that the ratio of information items used varies greatly between reporters and occurrences. Furthermore, the number of information pieces used in a report was related to the quality assessments made by the exercise management. The results, according to Lif et al., (2018), show that, while the general assessment of content relevance of the simplified cyber incident reporting template was favourable, the template still needs to be validated further.

RESEARCH METHODOLOGY

The views of experts were incorporated in the report on the evaluation of the effectiveness of the proposed CIHF for South African schools which was conducted using an expert review survey approach. The purpose of the survey was to ascertain experts' opinions on the proposed cyber incident handling framework (CIHF) for schools in South Africa. The rationale for using expert reviewers was to garner the expertise and knowledge of the reviewers (Tongco, 2007; Jansen and Hak, 2005). Richey and Klein (2014) stated that expert review is essential in validating research study outcomes. Expert reviews help to expose potential weaknesses concerning the subject under evaluation (Holbrook, Krosnick, Moore and Tourangeau, 2007). Expert reviews were also used by the researcher to facilitate a proper assessment of the study (Jansen and Hak, 2005).

A verification of the proposed CIHF for South African schools was conducted by the researcher using an expert review survey approach, which is known for its exploratory nature, focusing on the special knowledge of experts (Al-Sakkaf, 2019). Since the purpose of the expert reviews was to verify the framework, the researcher did not provide details about data collection and analysis (Maramwidze-Merrison, 2016). The main contribution of the expert review process was the documenting of expert opinions regarding the proposed CIHF for schools in South Africa. Ethical clearance regarding this framework evaluation was obtained from UNISA's CSET Ethics Review Committee. The survey was about 45 minutes. The questions were intended to evaluate the phases, stages, and comprehensiveness of the framework. What was essential to the researcher was to obtain confirmation from the experts that the proposed framework could contribute to dealing with cyber incidents in South African schools (Kortjan and van Solms, 2014). The framework was revisited and adapted, accordingly, based on the feedback that was received from the experts. The valued feedback and suggestions helped to make improvements to the framework.

IDENTIFYING EXPERT REVIEWERS

Holbrook et al. (2007) advocate that the number of expert reviewers used in an evaluation of a process should not be less than two and not more than five. Therefore, any number of experts between two and five is sufficient for an evaluation process. Nielsen (2000) supports Holbrook et al. (2007) by suggesting that five experts are sufficient to obtain good results, therefore, five experts were used to evaluate the framework. The expert reviewers were identified using a non-random selection and a purposive sampling technique (Russel, 2006; Bouma and Ling, 2004). The purposive sampling technique suggests that reviewers are chosen at the discretion of the researcher based on the requirements of the research (Tongco, 2007). Therefore, the researcher used purposive sampling to identify the expected reviewers to evaluate the framework.

To ensure that the sampling was impartial, selection criteria were used to identify the expert reviewers. The selection criteria that were used were, firstly, the qualification of the reviewers, secondly, their knowledge level within the research field, and, thirdly, their experience in the field of research (Richey and Klein, 2014). Experts in the fields of computing, computer science, information systems, ICT, or specialists in the research were selected. The minimum qualification level for the survey was a doctoral degree, with knowledge of what affects learners in cyberspace or who was an expert in research. Willingness to participate was the overall criterion that was considered. The expert reviewers who participated in the review are listed in Table 1. Their names have been excluded for ethical reasons.

TABLE 1
EXPERT REVIEWERS' SELECTION

Expert Reviewer	Qualification	Experience in the field	Knowledge Level (Role in the field of expertise)
1	PhD	**Researcher** More than 20 years' experience in the management of research, education, business, and government-related projects (including innovation and technology). More than 30 years advanced experience in higher education training, research, and scientific writing.	Consultant in technology and innovation, education and training, higher education management, policy development, postgraduate supervision professor (ICT department) and e-skills research coordinator (CoLab).
2	PhD	**Academic** More than 5 years in higher education and in an ICT department.	Associate Professor: Digital Transformation and Innovation. A postgraduate supervisor.
3	PhD	**Academic** More than 25 years' experience in higher education.	Research fellow for the National Research Foundation of South Africa (NRF). An author, a reviewer, an academic and postgraduate supervisor (medical physics, radiography, and applied physics).
4	PhD	**Researcher** Postdoctoral researcher with more than 5 years' experience in higher education.	Research fellow in the field of fourth industrial revolution on training and development in South Africa.
5	PhD	**Academic** Senior lecturer in the Department of Computer Science with more than 5 years of experience with higher education	The field of research is the next generation networks (TV white spaces and 5G), big data, game theory, indigenous knowledge systems, and ICT for development (ICT4D).

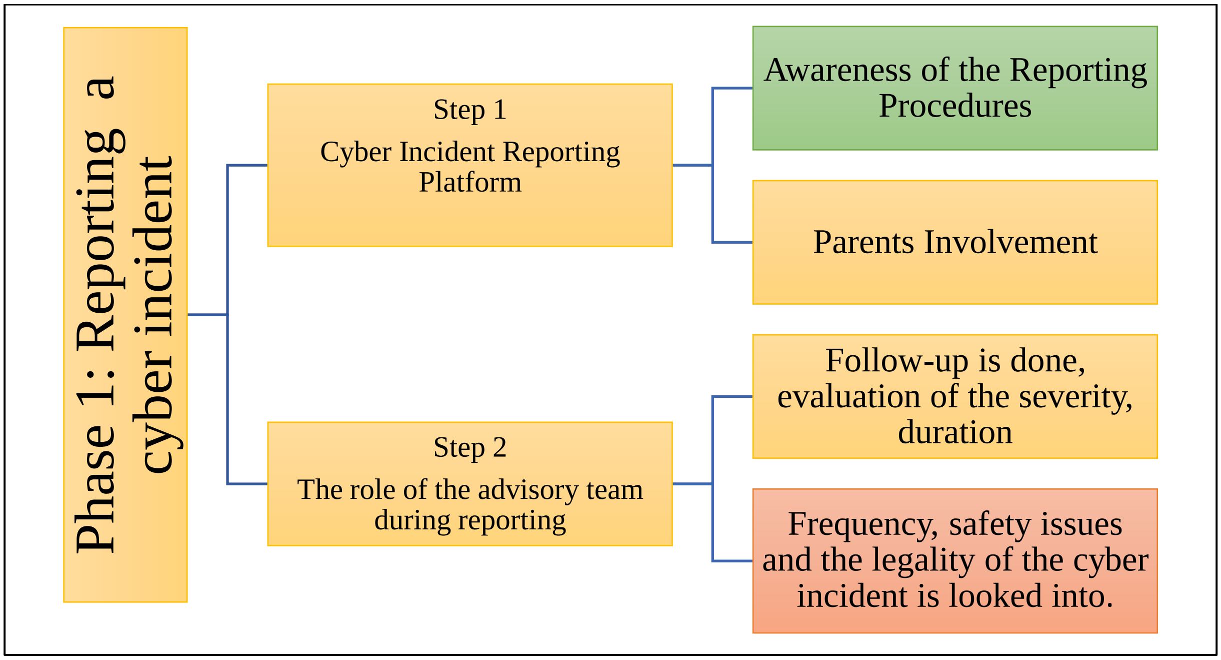
Source: Author's Analysis

Experts were invited to evaluate the comprehensiveness of the framework, as well as its applicability and relevance to South African schools. The experts were requested to rate the framework according to their own opinion, i.e., the information was gathered to garner the opinion of the experts. The review entailed completing an expert review survey about the CIHF, which was distributed electronically via Google Forms. Reviewers were initially contacted via telephone to facilitate an introduction to the researcher and the research study itself. After the introductions were made, the experts were invited to participate in the survey. Upon an expert's agreement to participate, they received additional information regarding the research study via email. The survey also contained a brief description of the study, as well as a detailed examination of the different elements of the framework, to assist the experts to gain a clear understanding of the context. Experts were assured of their anonymity during the process and their consent was acquired beforehand, although they had a choice to withdraw from the survey at any time.

THE OVERVIEW OF THE CYBER INCIDENT HANDLING FRAMEWORK

The cyber incident handling process is divided into four major phases; Reporting a Cyber Incident, Investigating Cyber Incidents, Post Investigation, and Review Process, and are depended on each other to produce a holistic approach.

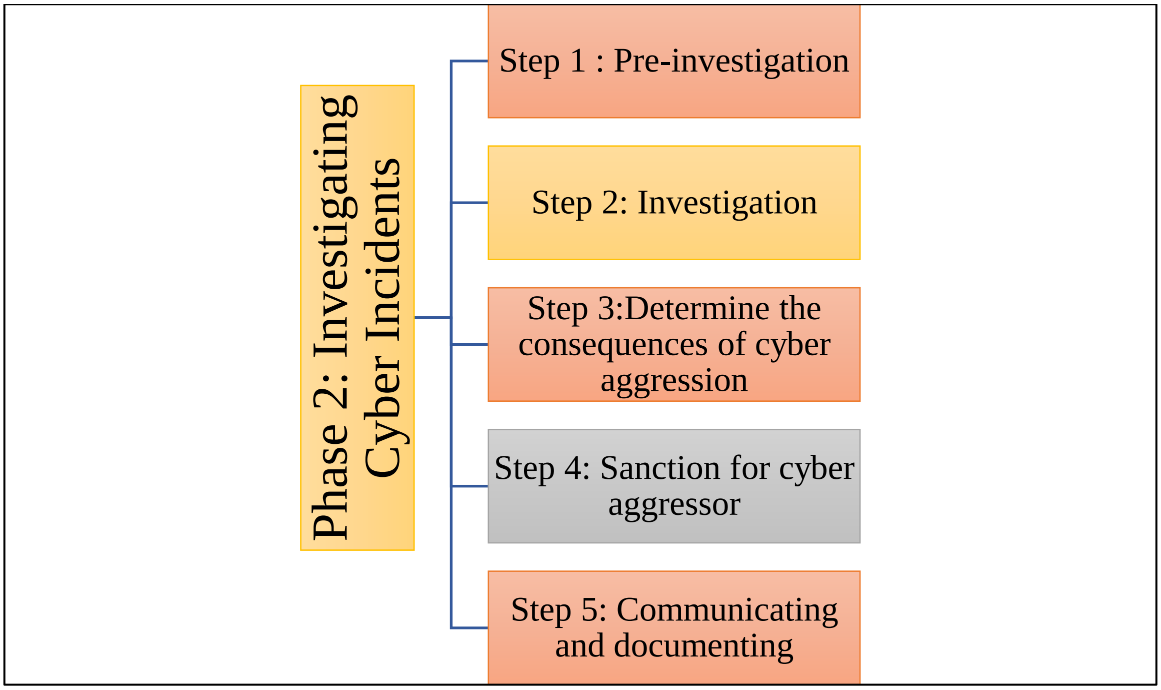
FIGURE 1
STEP ONE OF THE CYBER INCIDENT HANDLING FRAMEWORK


Phase 1: Reporting a cyber incident
Step 1
Cyber Incident Reporting Platform
Awareness of the Reporting Procedures
Parents Involvement
Step 2
The role of the advisory team during reporting
Follow-up is done, evaluation of the severity, duration
Frequency, safety issues and the legality of the cyber incident is looked into.

Source Authors' computation

The first phase of the cyber incident handling framework is the aspect of Reporting a Cyber Incident. This phase has two main steps which involve having a Cyber Incident Reporting Platform which focuses on Awareness of the Reporting Procedures and making sure that Parents are involved. The next step is outlining the Role of the Advisory Team during Reporting. These roles are important to ensure that follow-ups are maintained, it is also important to evaluate the severity, duration, frequency, safety concerns, and legality of the cyber incident in line with ICT policies and procedures. The second phase of the Cyber Incident Handling Framework entails Investigating Cyber Incidents as shown in figure 2.

FIGURE 2
STEP TWO OF THE CYBER INCIDENT HANDLING FRAMEWORK

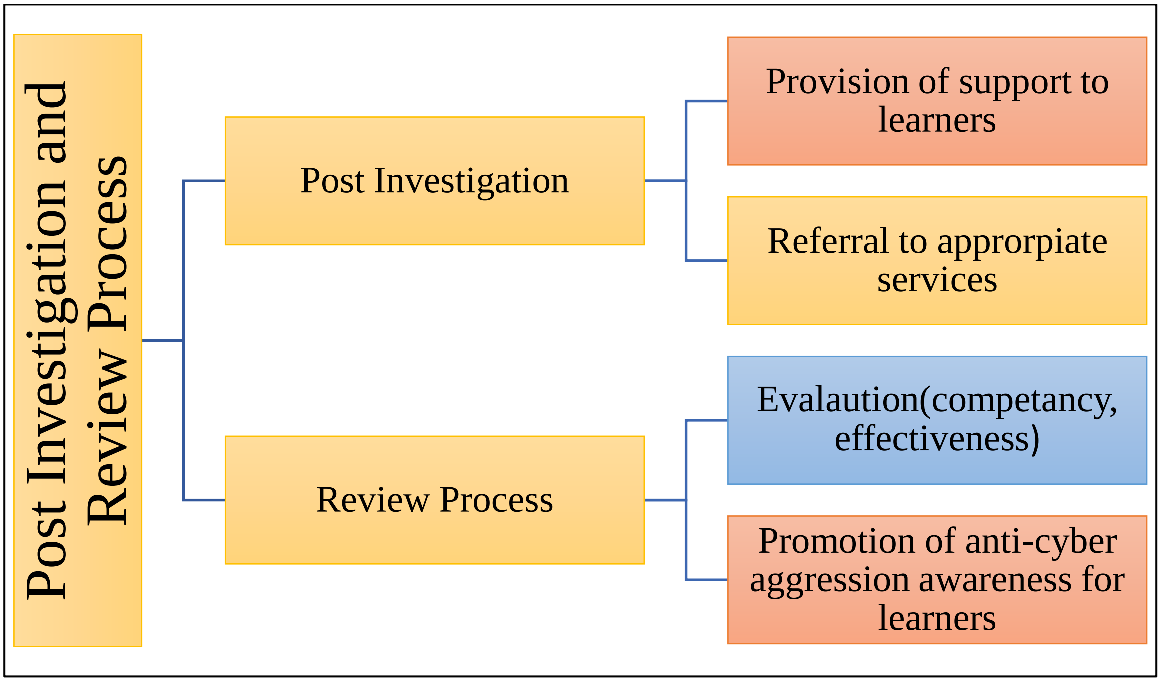

Phase 2: Investigating Cyber Incidents
Step 1 : Pre-investigation
Step 2: Investigation
Step 3:Determine the consequences of cyber aggression
Step 4: Sanction for cyber aggressor
Step 5: Communicating and documenting

Source: Author's Computation

Phase two of the cyber incident handing framework involves the investigation of cyber incidents with five stages which include Pre-Investigation where there should be: Support the Cyber Victim, Support the Bystanders. It also involves the Role players play their roles and Referral to appropriate services. Step 2 involves the Investigation where there should be Identifying the Aggressor, Seizing and Confiscating Electronic Items, Getting Information from Electronic Devices, and Capturing Digital Evidence. The final step is to Refer to appropriate services.

The third step involves the determination of the Consequences of Cyber Aggression which include a Breach of School Rules and Regulations, Suspected E-Crime, Child Protection Issues. At this point schools should have school ICT policy directly aimed at regulating cyber aggression in schools, Codes of Conduct should be formulated and adopted, Referral to appropriate services, schools should comply with cyber legislation which applies to schools and learners and Schools should comply with law enforcement. Step four involves sanctioning the cyber aggressor by referring them to the appropriate services and communicating and documenting as the final step. The third and fourth phases involve the process of Post Investigation and Review process.

FIGURE 3
THE PROCESS OF POST INVESTIGATION AND REVIEW PROCESS

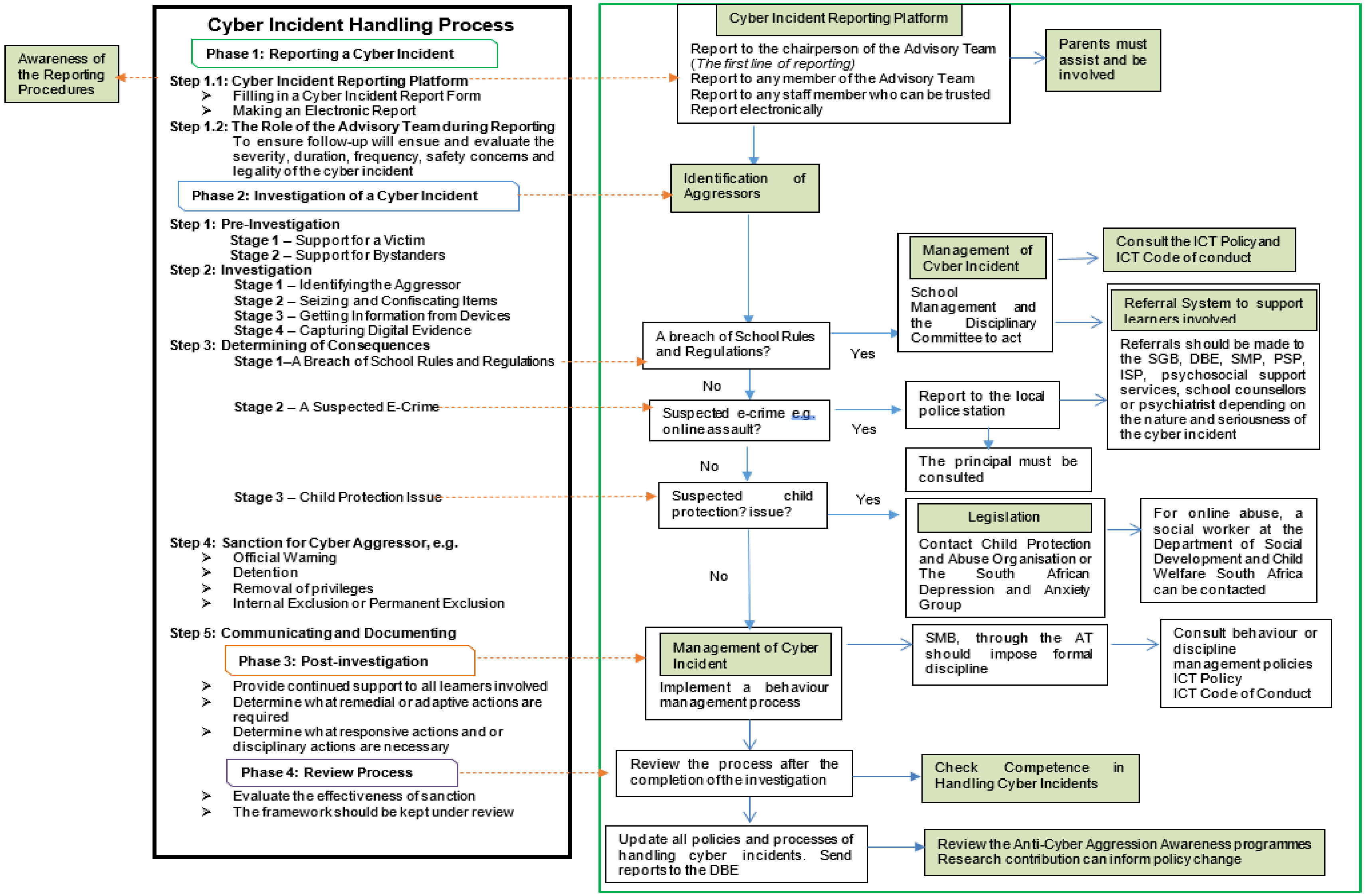

Post Investigation and Review Process
Post Investigation
Review Process
Provision of support to learners
Referral to approrpiate services
Evalaution(competancy, effectiveness)
Promotion of anti-cyber aggression awareness for learners

In figure 3, Post Investigation involves the need to provide continued support to all learners involved, determine what remedial or adaptive actions are required, and determine what responsive actions or disciplinary actions are necessary. Referral to appropriate services is also critical. The final phase is the review process where there is a need to evaluate the effectiveness of sanction and competence in handling cyber incidents and Promote Anti-Cyber Aggression Awareness for learners. The overall integration of the cyber handing framework is outlined in figure 4.

THE CYBER INCIDENT HANDLING FRAMEWORK

In figure 4 the overall integration of the cyber incident handling process (phases, steps and stages) and a flow diagram of a decision-making procedure is presented. The overall integration is outlining the proposed CIHF. The decision-making procedure illustrates the processes to be followed when a cyber incident occurs and the procedures to be considered when assisting learners. The safety and welfare of learners must be considered paramount throughout the process. The framework applies to all schools and can be implemented by the schools themselves according to the special needs of learners.

FIGURE 4
THE OUTLINE OF THE CYBER INCIDENT HANDLING FRAMEWORK


Awareness of the Reporting Procedures
Cyber Incident Handling Process
Phase 1: Reporting a Cyber Incident
Step 1.1: Cyber Incident Reporting Platform
➢ Filling in a Cyber Incident Report Form
➢ Making an Electronic Report
Step 1.2: The Role of the Advisory Team during Reporting
To ensure follow-up will ensue and evaluate the severity, duration, frequency, safety concerns and legality of the cyber incident
Phase 2: Investigation of a Cyber Incident
Step 1: Pre-Investigation
Stage 1 – Support for a Victim
Stage 2 – Support for Bystanders
Step 2: Investigation
Stage 1 – Identifying the Aggressor
Stage 2 – Seizing and Confiscating Items
Stage 3 – Getting Information from Devices
Stage 4 – Capturing Digital Evidence
Step 3: Determining of Consequences
Stage 1–A Breach of School Rules and Regulations
Stage 2 – A Suspected E-Crime
Stage 3 – Child Protection Issue
Step 4: Sanction for Cyber Aggressor, e.g.
➢ Official Warning
➢ Detention
➢ Removal of privileges
➢ Internal Exclusion or Permanent Exclusion
Step 5: Communicating and Documenting
Phase 3: Post-investigation
➢ Provide continued support to all learners involved
➢ Determine what remedial or adaptive actions are required
➢ Determine what responsive actions and or disciplinary actions are necessary
Phase 4: Review Process
➢ Evaluate the effectiveness of sanction
➢ The framework should be kept under review
Cyber Incident Reporting Platform
Report to the chairperson of the Advisory Team
(The first line of reporting)
Report to any member of the Advisory Team
Report to any staff member who can be trusted
Report electronically
Parents must assist and be involved
Identification of Aggressors
A breach of School Rules and Regulations?
Yes
No
Management of Cyber Incident
School Management and the Disciplinary Committee to act
Consult the ICT Policy and ICT Code of conduct
Referral System to support learners involved
Referrals should be made to the SGB, DBE, SMP, PSP, ISP, psychosocial support services, school counsellors or psychiatrist depending on the nature and seriousness of the cyber incident
Suspected e-crime e.g. online assault?
Yes
No
Report to the local police station
The principal must be consulted
Suspected child protection? issue?
Yes
No
Legislation
Contact Child Protection and Abuse Organisation or The South African Depression and Anxiety Group
For online abuse, a social worker at the Department of Social Development and Child Welfare South Africa can be contacted
Management of Cyber Incident
Implement a behaviour management process
SMB, through the AT should impose formal discipline
Consult behaviour or discipline management policies
ICT Policy
ICT Code of Conduct
Review the process after the completion of the investigation
Check Competence in Handling Cyber Incidents
Update all policies and processes of handling cyber incidents. Send reports to the DBE
Review the Anti-Cyber Aggression Awareness programmes
Research contribution can inform policy change

The researcher proposed and developed a CIHF that will assist schools with procedures when handling cyber incidents. The framework is intended to provide a guide to reporting cyber incidents and to direct all role players toward appropriate reporting procedures and intervention processes. The framework provides a systematic approach to ensure that each role player plays their role to assist learners. The framework focuses on making the mechanisms of investigations and responses more transparent and the reports of cyber incidents more appropriately and consistently investigated.

THE GENERAL ANALYSIS OF THE EXPERT FEEDBACK

Five expert reviewers who met the selection criteria were willing to participate in evaluating and validating the proposed framework, which was done through an online survey using Google Forms. The feedback and reaction to the feedback are as indicated in the following sections.

THE CLARITY OF RESEARCH OVERVIEW

A general overview of the research was presented to the experts in a form of a diagram. The experts were requested to comment on the clarity of the overview of the research. The experts indicated that the overview of the research was relatively and sufficiently clear. A relevant suggestion that was highlighted was that it would suffice for the literature to include general cyber safety framework standards. The suggestion was adopted. Another expert suggested that a superficial idea about the inclusion criteria into focus groups may make the procedure clearer to non-expert readers, as the outcomes of this research are meant to influence policy formulation. This suggestion was adopted. The last recommendation was the inclusion of a business continuity plan for schools. The concept of business continuity management and planning was included in the research.

THE NEEDS FOR ADDRESSING CYBER INCIDENTS

The experts were presented with the need for addressing cyber incidents in South African schools. The needs were the result of a critical literature review that was done focusing on the prevalence and impact of cyber incidents among learners. The experts were requested to suggest any other needs to be included in the list. According to the experts, the list of needs presented and summarised was comprehensive, the coverage of the needs was well articulated and it was appreciated that the list can never be exhaustive. One of the experts emphasised the psychological impact of cyber incidents on the lives of learners and the need for an educational psychologist to assist learners who are affected by cyber incident ordeals. The aspect of a psychologist was included in the research.

SUGGESTION ON SUPPORT STRUCTURES

The support structures and the role players and their responsibilities were presented to the experts. According to the experts, the support structures presented were sufficient because all the important stakeholders were included. One important suggestion that was highlighted was the issue of boarding schools, as these schools have their unique situations regarding exposure to cyber incidents and potential immediate support structures. A comment was made in this regard that boarding school staff members should assist in monitoring and reducing cyber incidents. On a different note, the experts appreciated the inclusion of overarching support from the central government because the framework includes schools at the national level, thus the central role of government is critical to the effective implementation of cyber incident procedures. Policies for schools are instructions from the Department of Basic Education (DBE) and are meant to filter down to school management for implementation.

THE NEEDS FOR ADDRESSING CYBER INCIDENTS AND ROLE PLAYERS

A table that outlines the link between the needs and the respective role players was presented to the experts. The experts were requested to indicate whether there was any information to be added to the table. The experts indicated that the table summarised the most important needs and role players and that it was quite comprehensive. The experts also indicated that, while the list cannot be exhaustive, the critical issues were well articulated. The experts appreciated the fact that the table highlighted the views of learners on cyber incidents. One expert recommended that the documentation of all advisory team's (AT) activities, especially the investigation, the determination of consequences, and the review process, as well as the reliable timeline for the execution of each stage in the framework, should be part of the framework. The suggestion was addressed. Another suggestion from the experts was that learners should be aware of what constitutes appropriate online behavior, the availability of filtering and blocking software at school to prevent access to inappropriate content. The information on what constitutes appropriate online behavior was highlighted, where learners are reminded of online behavior in cyberspace. Lastly, it was noted that parental involvement might be a challenge, as this will depend on the age of a learner. However, efforts should still be made to assist learners.

FEEDBACK ANALYSIS USING A LIKERT SCALE

The experts were requested to evaluate the importance and relevance of the proposed tables, processes, phases, and overall framework. Firstly, the analysis focused on how the findings from the focus group interviews were evaluated. The experts were invited to rate the tables according to their importance to the CIHF. The experts rated the tables according to their own opinions, based on a four-point Likert scale of Very Important; Neutral Important; Low Importance; and Not Important. A Likert scale can be used in research to determine feedback from expert reviewers (Allen and Seaman, 2007). Secondly, the analysis focused on how the pillar processes and the phases were rated according to their importance to the CIHF. Finally, the experts were requested to rate the overall importance of the framework to South African schools. All the ratings used a four-point Likert scale.

The interval scale used does not represent any form of quantitative scale difference between each point and is thus considered an ordinal scale (Joshi, Kale, Chandel and Pal, 2015). Allen and Seaman (2007) defined an ordinal scale as data presented in an ordering or ranking manner as per the responses but no measure of distance is probable. Table 2 indicates the results of the expert reviews of the proposed tables, processes, phases, and the overall framework.

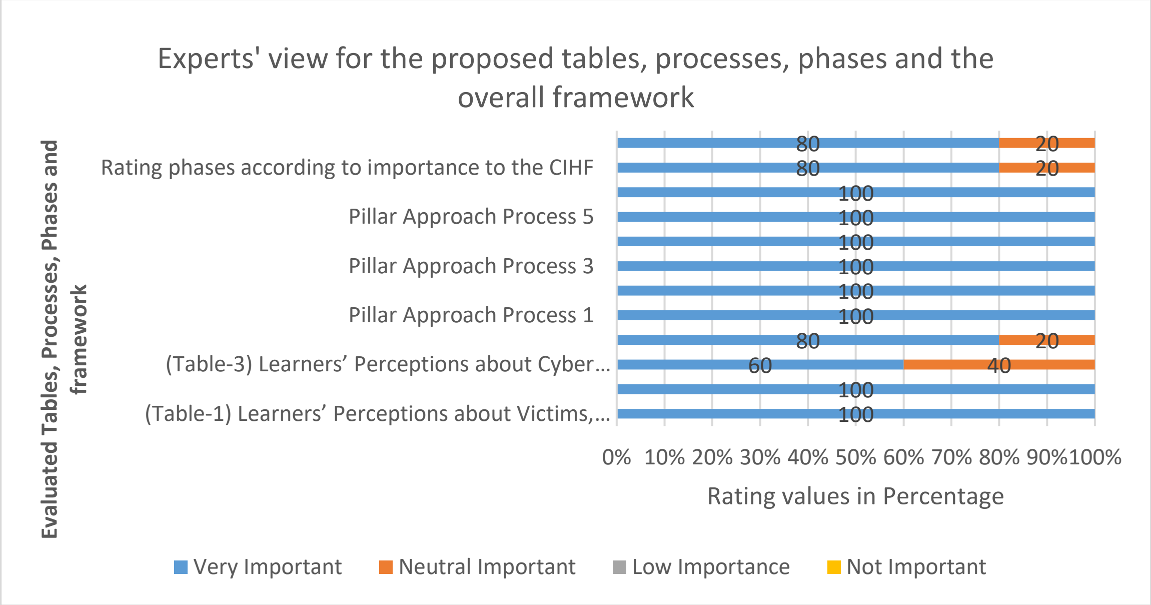
TABLE 2
EVALUATED TABLES, PROCESSES, PHASES, AND THE OVERALL FRAMEWORK

Evaluated tables, processes, phases, and the overall framework		Very Important	Neutral Important	Low Importance	Not Important
Rating tables according to importance to be included in the framework (tables)	(Table-1) Learners' Perceptions of Victims, Aggressors and Bystander	5 $^{(1,2,3,4,5)}$	-	-	-
	(Table-2) Learners' Perceptions of Technology	5 $^{(1,2,3,4,5)}$	-	-	-
	(Table-3) Learners' Perceptions of Cyber Incidents	3 $^{(1,2,5)}$	2 $^{(3,4)}$	-	-

	(Table-4) Learners' Perceptions of Adults	4 (1,2,4,5)	1 (3)	-	-
Rating processes according to importance to the CIHF	Pillar Approach Process 1	5 (1,2,3,4,5)	-	-	-
	Pillar Approach Process 2	5 (1,2,3,4,5)	-	-	-
	Pillar Approach Process 3	5 (1,2,3,4,5)	-	-	-
	Pillar Approach Process 4	5 (1,2,3,4,5)	-	-	-
	Pillar Approach Process 5	5 (1,2,3,4,5)	-	-	-
	Pillar Approach Process 6	5 (1,2,3,4,5)	-	-	-
Rating phases according to importance to the CIHF	Rating phases according to importance to the CIHF	4 (1,2,3,5)	1 (4)	-	-
Rating the importance of the CIHF	Rating the importance of the CIHF	4 (1,2,3,4)	1 (5)	-	-

The Likert scale values for Table 2 were presented in a 100% stacked bar chart in Figure 2.

FIGURE 5
100% STACKED BAR CHART FOR THE TABLES, PROCESSES, PHASES, AND THE OVERALL FRAMEWORK



The Likert-scale data was converted to numeric values to enable the researcher to calculate a single average response, thus making it easier to analyse the feedback on the tables, processes, phases and the overall framework (Sullivan and Artino Jr, 2013; Likert, 1932). The Likert scale data were converted to a numerical value using a point system. The numerical values assigned were: Not Important = 1; Low Importance = 2; Neutral Important = 3; and Very Important = 4. Table 7-3 shows an example of how the average agreement value was calculated.

TABLE 3
THE CALCULATION OF AN AVERAGE AGREEMENT VALUE

(Table-3) Learners' Perceptions of Cyber Incidents				
Number of experts	Rating level		Points for each level	Total points from the experts
3	Very Important	X	4 points	= 12
2	Neutral Important	X	3 points	= 6
0	Low Importance	X	2 points	= 0
0	Not Important	X	1 point	= 0
				18 Points / 5 experts that answered the survey = **3.6 Average for Table 3**

The average agreement values were used to compare outcomes instead of relying on elusive aspirations. The average agreement values were calculated to give numbers that describe the experts' sentiments. An average agreement value for a question gives a sentiment score for the entire question. Table 4 shows the average agreement values for reviewers' assessment of the tables, processes, phases, and the overall framework.

TABLE 4
AVERAGE AGREEMENT VALUES FOR THE TABLES, PROCESSES, PHASES, AND FRAMEWORK

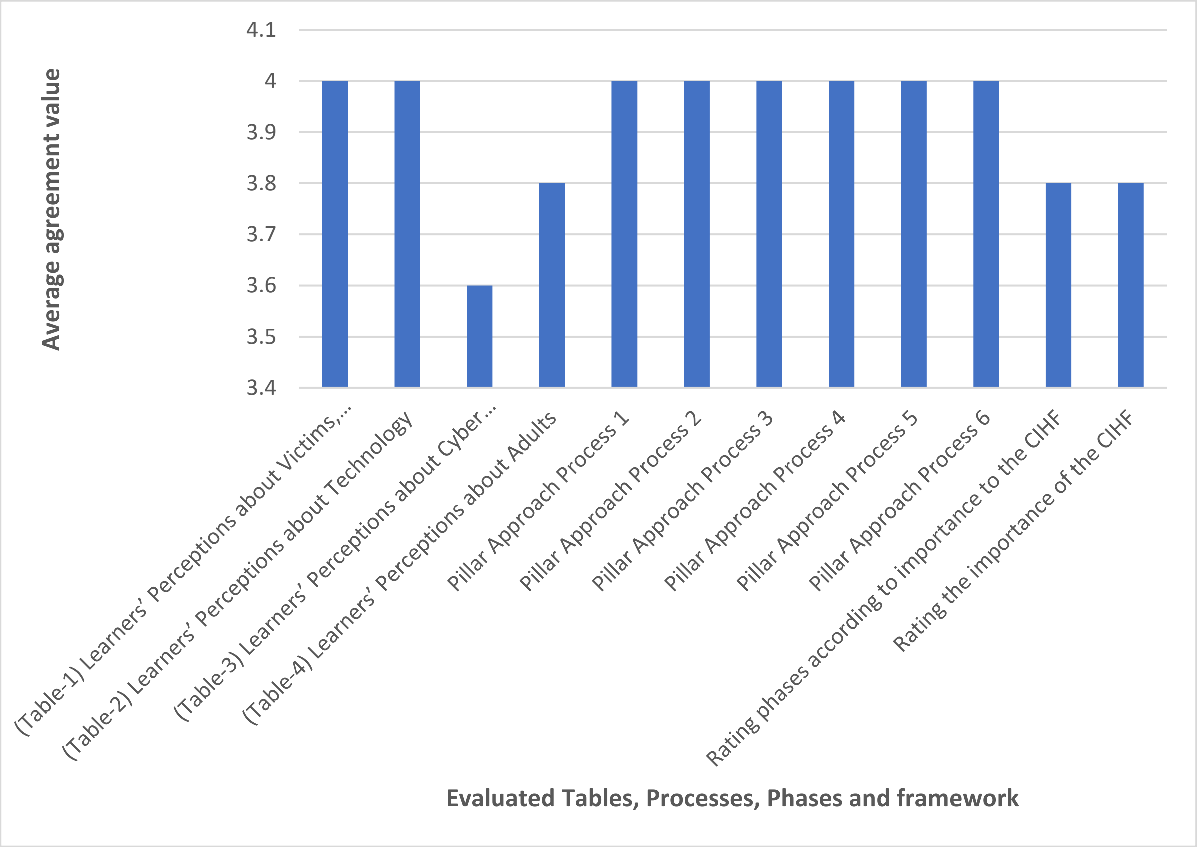
Evaluated tables, processes, phases, and the overall framework		Average agreement value (n=4)
Rating tables according to importance to be included in the framework (tables)	(Table-1) Learners' Perceptions of Victims, Aggressors and Bystander	4
	(Table-2) Learners' Perceptions of Technology	4
	(Table-3) Learners' Perceptions of Cyber Incidents	3.6
	(Table-4) Learners' Perceptions of Adults	3.8
Rating processes according to importance to the CIHF	Pillar Approach Process 1	4
	Pillar Approach Process 2	4
	Pillar Approach Process 3	4
	Pillar Approach Process 4	4
	Pillar Approach Process 5	4
	Pillar Approach Process 6	4
Rating phases according to importance to the CIHF	Rating phases according to importance to the CIHF	3.8
Rating the importance of the CIHF	Rating the importance of the CIHF	3.8

It was easier for the researcher to compare the length and position, on the bar chart. The average agreement value per rating is presented in Figure 3.

The tables (the proposed conceptual framework) were evaluated according to their importance to the CIHF. The tables represented the themes that were generated from the focus group interviews and the reviewed literature. The tables had an average agreement value rating of 3.6 points and above. Thus, the reviewers considered the tables to be “Neutral Important” to “Very Important”. The tables were rated as important, vital, and relevant because they draw attention to the views of learners on cyber incidents in South African schools.

Figure 6 indicates that the average agreement rating for the processes is 4 points and, thus, the reviewers considered the processes to be vital parts of the framework. The experts were content with the collation and flow of information within the processes. They indicated that the identified processes and pillars are important and that they contribute to the comprehensiveness of the framework. The researcher was commended for identifying important pillars and for coming up with an easily adaptable framework. The average rating of the phases was 3.8 points, i.e., “Neutral Important”. The experts felt that the phases were vital and relevant as parts of the framework. Comments about the clarity and usefulness of the phases to the framework were that the phases are well synchronized, clear, comprehensive, and useful and that each step and phase was presented with clarity. One of the experts applauded the framework for providing an immediate and temporary solution, while a comprehensive evidence-based solution is being worked out.

FIGURE 6
AN AVERAGE AGREEMENT VALUES FOR THE TABLES, PROCESSES, PHASES, AND FRAMEWORK

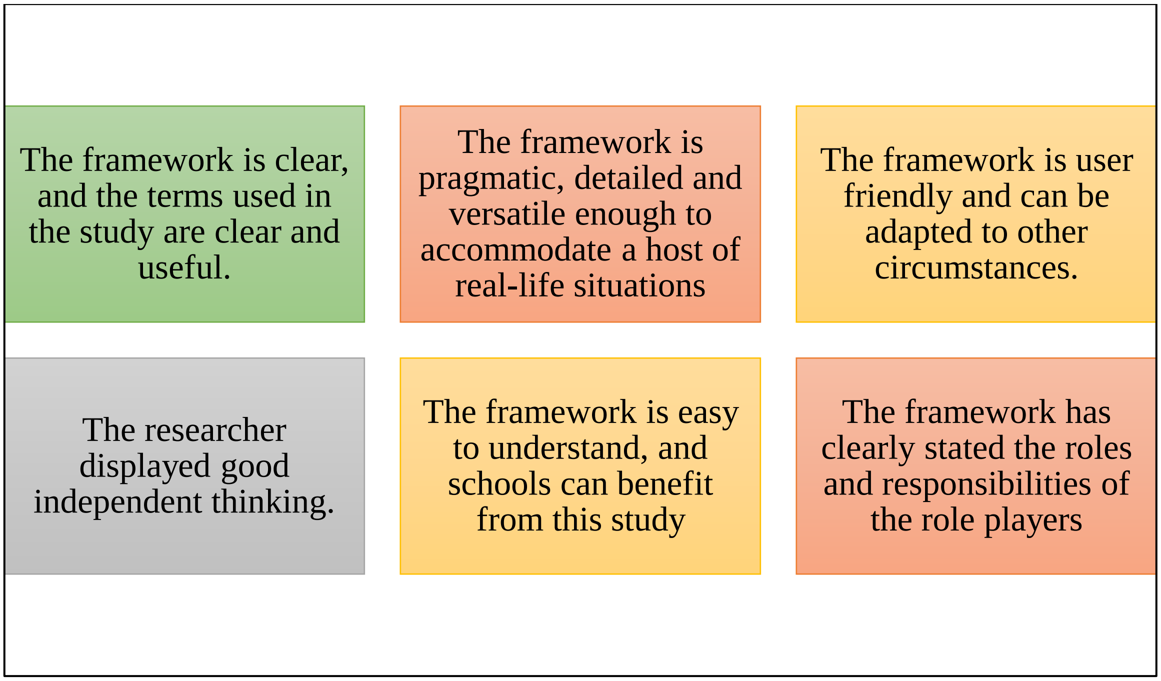


The average agreement rating for the importance of the CIHF was 3.8 points, i.e., “Neutral Important”. Comments given by the experts were that the content, flow of information, and the overall outline of the framework were clear and were presented professionally. The overall outline was comprehensive, with the important aspects of the framework covered.

THE OVERALL CLARITY, EASE-OF-USE, AND ADAPTABILITY OF THE FRAMEWORK

The experts were requested to give their views on the overall clarity, ease of use, and adaptability of the framework. Their comments are indicated in the figure below:

FIGURE 7
THE OVERALL CLARITY, EASE-OF-USE, AND ADAPTABILITY OF THE FRAMEWORK



The framework is clear, and the terms used in the study are clear and useful.

The framework is pragmatic, detailed and versatile enough to accommodate a host of real-life situations

The framework is user friendly and can be adapted to other circumstances.

The researcher displayed good independent thinking.

The framework is easy to understand, and schools can benefit from this study

The framework has clearly stated the roles and responsibilities of the role players

Figure five is outlining the views of experts on the framework, the experts believe that the framework is clear, and the terms used in the study are clear and useful, the framework is pragmatic, detailed, and versatile enough to accommodate a host of real-life situations, the framework is user friendly and can be adapted to other circumstances, the researcher displayed good independent thinking, the framework is easy to understand, and schools can benefit from this study and the framework has clearly stated the roles and responsibilities of the role players.

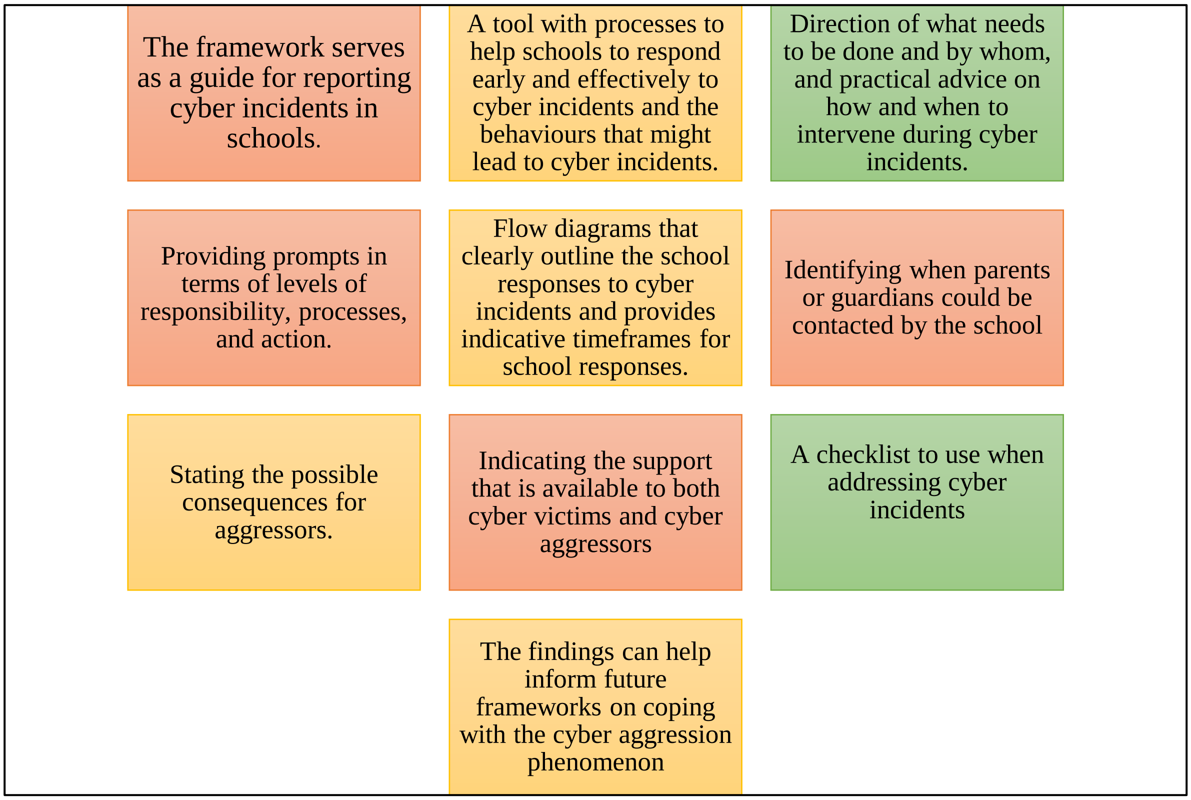
CHALLENGES IN IMPLEMENTING THE FRAMEWORK

The experts were requested to indicate whether they foresaw any major challenges in implementing the framework and how the challenges could be addressed. Some challenges were highlighted: The implementation of the framework might require resources, and this can be solved by ensuring that the government and the private sectors come together in implementing the framework. The proposed framework is ideal, but it might take some time to fully implement the framework, with the possibility of all role players eventually becoming involved as proposed by the framework. One expert was concerned about how feasible it will be to try and involve e.g., law enforcement, social media platform providers/companies, etc., role players who are outside the school. There should be a buy-in from all role players. It might not be feasible to implement all the phases in the short term, given that some of the role players are completely independent of the schools, learners, and DBE. It might also take time to convince certain role players to take part.

THE CONTRIBUTION OF THE FRAMEWORK

The CIHF contributed to the academic body of knowledge in the field of cyber safety in schools in that:

FIGURE 8
THE CONTRIBUTION OF THE FRAMEWORK



The framework serves as a guide for reporting cyber incidents in schools.

A tool with processes to help schools to respond early and effectively to cyber incidents and the behaviours that might lead to cyber incidents.

Direction of what needs to be done and by whom, and practical advice on how and when to intervene during cyber incidents.

Providing prompts in terms of levels of responsibility, processes, and action.

Flow diagrams that clearly outline the school responses to cyber incidents and provides indicative timeframes for school responses.

Identifying when parents or guardians could be contacted by the school

Stating the possible consequences for aggressors.

Indicating the support that is available to both cyber victims and cyber aggressors

A checklist to use when addressing cyber incidents

The findings can help inform future frameworks on coping with the cyber aggression phenomenon

Figure 8 is showing the contribution of the framework which includes that the framework serves as a guide for reporting cyber incidents in schools, a tool with processes to help schools to respond early and effectively to cyber incidents, and the behaviors that might lead to cyber incidents. The framework shows the direction of what needs to be done and by whom, and practical advice on how and when to intervene during cyber incidents, providing prompts in terms of levels of responsibility, processes, and action. The framework provides flow diagrams that clearly outline the school responses to cyber incidents and provides indicative timeframes for school responses, identifying when parents or guardians could be contacted by the school’ The framework states the possible consequences for aggressors, indicating the support that is available to both cyber victims and cyber aggressors. The framework provides a checklist to use when addressing cyber incidents and the findings can help inform future frameworks on coping with the cyber aggression phenomenon.

RECOMMENDATIONS FOR THE FRAMEWORK TO BE USED IN SCHOOLS

The experts commended the framework as unique and that it could be used in schools because it brings all the stakeholders together. The framework could be used as a guide to solving cyber incident problems in schools and it is a step in the right direction. When processes for reporting and supporting learners are established, cyber incidents can be reduced before they escalate or go viral. Timely intervention to alleviate the plight of the victims may make a difference between life and death. The feedback from the experts indicated that the framework was relevant and important in dealing with cyber incidents in South African schools.

The implementation of this framework will provide South African schools with procedures to follow when intervening during cyber incidents. Implementing procedures that encourage learners to respect each other online remains an important responsibility of the school. The framework is designed to be flexible and to allow schools to use parts of it that are relevant to their own needs. The framework applies to all schools and can be implemented by the schools themselves, according to the special needs of their learners and in line with Department of Basic Education (DBE) policies, plans, and procedures. The procedures and steps are not meant to constitute an additional burden but are meant to serve as management tools to help schools incorporate cyber safety issues into school management, processes, and activities. The framework is only as good as the degree to which it is implemented and monitored over time. The overall goal of the framework is to create a supportive learning environment for learners, educators, principals, school governing bodies, and administrators and, in so doing, retain learners in schools. The framework is not a complete solution to all cyber aggression problems in schools, but it represents a starting point to enhance the reporting of cyber incidents in South African schools. The framework can be used in conjunction with other existing physical bullying frameworks, as a supplement to reporting procedures in schools.

FUTURE IMPROVEMENTS ON THE FRAMEWORK FOR IMPLEMENTATION

The future improvements to the framework were highlighted by the reviewers:

- The issue of the framework is a bit victim-friendly was highlighted, this can be addressed by taking into consideration the challenges of aggressors.
- For implementation, a less technical modular framework, alongside the technical framework, should be provided. Some steps involving independent role players might also be refined to increase the feasibility of complete framework adoption or implementation.
- Create a more detailed document for each of the phases and steps to provide a low-level, step-by-step process for the implementation. This will provide schools with additional information and an implementation guide on how the proposed framework can be implemented.
- The implementation by non-technical personnel may need to be preceded by a low-level workshop because the implementation of the framework might present unforeseen challenges and it might take a bit of convincing other external role players.
- The increased use of and dependence on new cyberspace technologies is creating new risks, particularly human factor risks, therefore, there is a need for more research to address the new risks.

As ICT use is likely to increase and become more 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. Efforts to prevent cyber incidents in schools should become part of a more comprehensive approach to bullying prevention and intervention. It emerged from this study that the following areas or topics require more research:

- Empirical research should continue to be conducted to understand the cyber incident phenomenon in South African schools, as well as develop evidence-based intervention programs to control and combat cyber incidents.
- More qualitative research is needed to provide opportunities for the cyber incident aggressors to highlight their perceptions and experiences.

CONCLUSION AND POLICY RECOMMENDATIONS

The goal of this research was to develop a Cyber Incident Handling Framework (CIHF) for South African schools to improve their effectiveness in dealing with cyber incidents while also ensuring that each role player is involved in the intervention process aimed at reducing cyber incidents in schools. An expert review survey was used to elicit feedback on the proposed cyber incident handling framework (CIHF) for schools in South Africa. The use of expert reviewers was justified to benefit from the expertise and knowledge of the reviewers. The expert opinion helped establish the usefulness of the proposed framework, reflecting on its quality, and determining how effectively it supports the solution of reporting cyber occurrences in South African schools. The documenting of expert opinion on the intended CIHF for South African schools was a key contribution to the expert review process. The study outlined the Cyber Incident Handling Framework (CIHF), as well as the issues associated with its implementation and how they can be addressed. According to existing research, South Africa has few mechanisms in place for dealing with cyber occurrences that are consistently followed by schools. This scarcity hurts the transparency, appropriateness, and consistency of inquiry and response processes in the event of a cyber incident.

A Cyber Incident Handling Framework (CIHF) was developed and recommended for South African schools to improve the effectiveness of handling cyber incidents while also ensuring that each role participant has a significant role to play in the intervention process aimed at reducing cyber incidents in schools. When this framework is implemented, South African schools will have processes to follow when dealing with cyber incidents. The school must continue to implement practices that encourage learners to treat one another with respect online. The framework is meant to be adaptable, allowing schools to employ aspects of it that are relevant to their specific needs. The framework applies to all schools and can be implemented by the schools themselves, by Department of Basic Education (DBE) policies, plans, and procedures, and according to the unique needs of their learners. The procedures and actions are not intended to add to the workload; rather, they are intended to be used as management tools to assist schools in incorporating cyber safety concerns into their school management, processes, and activities. The framework is just as effective as how well it is implemented and tracked over time. The framework's main purpose is to establish a conducive learning environment for learners, educators, principals, school governing bodies, and administrators, to keep learners in school. The framework is not a perfect solution to all cyber aggression issues in schools, but it is a good place to start if you want to improve how cyber incidents are reported in South African schools. As a supplement to school reporting procedures, the framework can be utilized in conjunction with other current physical bullying frameworks.

REFERENCES

Adom, D., Hussein, E.K., & Agyem, J.A. (2018). Theoretical and conceptual framework: Mandatory ingredients of a quality research. *International Journal of Scientific Research*, *7*(1), 158–172.

Allen, I.E., & Seaman, C.A. (2007). Likert scales and data analyses. *Quality progress*, *40*(7), 64–65.

Al-Sakkaf, N. (2019). *Of ambition, opportunity and pretense: The Politics of Gender in Yemen*. University of Reading.

Arundale Primary School. (2019). *Business Continuity Plan*. Retrieved September 30, 2021, from https://www.arundaleprimary.co.uk/business-continuity-plan/

Bouma, D., & Ling, R. (2004). *The Research Process*. Oxford University Press.

Centre for Justice and Crime Prevention and DBE. (2015). *The National School Safety Framework.* Cape Town.

Chi, M.T., Glaser, R., & Farr, M.J. (2014). *The nature of expertise*. Psychology Press.

Childnet International. (2016). *Cyberbullying: Understand, Prevent, and Respond - Guidance for schools*. London.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1–147.

Cilliers, L., & Chinyamurindi, W. (2020). Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa. *The Electronic Journal of Information Systems in Developing Countries*, *86*(4), e12131.

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*. Published by the Department of Basic Education.

EU. (2017). Klicksafe.de. Retrieved March 26, 2018, from http://www.klicksafe.de/

Goodyear, V. (2020). Narrative Matters: Young People, Social Media and Body Image. *Child and Adolescent Metal Health*, *25*(1), 48–50.

Goran, I. (2017). *Cyber security risks in public high schools*.

Gov.UK. (2017). *Uk council for child internet safety (ukccis)*. Retrieved February 15, 2018, from https://www.gov.uk/

Hettema, H. (2021). Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence. *Computers & Security*, *109*, 102396.

Holbrook, A.L., Krosnick, J.A., Moore, D., & Tourangeau, R. (2007). Response order effects in dichotomous categorical questions presented orally: The impact of question and respondent attributes. *Public Opinion Quarterly*, *71*(3), 325–348.

Jansen, H., & Hak, T. (2005). The productivity of the three-step test-interview (TSTI) compared to an expert review of a self-administered questionnaire on alcohol consumption. *Journal of Official Statistics*, *21*(1), 103.

Joshi, A. et al. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, *7*(4), 396.

Kortjan, N., & van Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), 29–41.

Kortjan, N., & Von Solms, R. (2013). *A cyber security awareness and education framework for South Africa* (Doctoral dissertation, Nelson Mandela Metropolitan University).

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, *28*(1), 1–17.

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, *29*(2), 16–35.

Kritzinger, E. (2020). Improving Cybersafety Maturity of South African Schools. *Information*, *11*(10), 471. https://doi.org/10.3390/info11100471

Lif, P., Sommestad, T., & Granasen, D. (2018, June). Development and evaluation of information elements for simplified cyber-incident reports. In *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)* (pp. 1–10). IEEE.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, *22*(140), 5–55.

Maclellan, E., & Soden, R. (2003). Expertise, expert teaching and experienced teachers' knowledge of learning theory. *Scottish Educational Review*, *35*(2), 110–120.

Maramwidze-Merrison, E. (2016). Innovative Methodologies in Qualitative Research: Social Media Window for Accessing Organisational Elites for interviews. *The Electronic Journal of Business Research Methods*, *12*(2), 157–167.

Mhlanga, D. (2020). Industry 4.0: The challenges associated with the digital transformation of education in South Africa. *The Impacts of Digital Transformation*, *13*.

Mhlanga, D. (2021). The Fourth Industrial Revolution and COVID-19 Pandemic in South Africa: The Opportunities and Challenges of Introducing Blended Learning in Education. *Journal of African Education*, *2*(2), 15–43.

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

Nielsen, J. (2000). *Why You Only Need to Test with 5 Users*. Nielsen Norman Group. Retrieved April 19, 2021, from https://www.nngroup.com/articles/why-you-need-to-test-with-5-users/.

Peffers, K. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68–74.

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

Rahman, N., Sairi, I., Zizi, N., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382.

Richardson, M.D., Lemoine, P.A., Stephens, W.E., & Waller, R.E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23–39.

Richey, R.C., & Klein, J.D. (2014). *Design and development research Handbook of research on educational communications and technology*. Springer.

Russel, B.H. (2006). *Research Methods in Anthropology: Qualitative and Quantitative Methods*. Rowman & Littlefield Publishers.

Smith, P.K. (2012). *Cyberbullying and cyber aggression*. Routledge.

Sonhera, N., Kritzinger, E., & Loock, M. (2021). Roles and Responsibilities for School Role Players in Addressing Cyber Incidents in South Africa. *Eurasian Journal of Social Sciences*, *9*(3), 123–137.

Sullivan, G.M., & Artino, A.R., Jr. (2013). Analyzing and interpreting data from Likert-type scales. *Journal of Graduate Medical Education*, *5*(4), 541–542.

Tokunaga, R.S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, *26*(3), 277–287.

Tongco, M.D. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications*, *5*(2007), 147–158.