Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute
InformingScience.org

IJIKM.org

Volume 20, 2025

TOWARDS A CYBERSAFETY COMMUNITY OF PURPOSE IN MARGINALISED SCHOOLS

Caroline Magunje*	University of Cape Town, Cape Town, South Africa	caroline.magunje@uct.ac.za
Wallace Chigona	University of Cape Town, Cape Town, South Africa	wallace.chigona@uct.ac.za
Baby Inneth Makofane	University of Limpopo, Polokwane, South Africa	inneth.makofane@ul.ac.za

* Corresponding author

ABSTRACT

Aim/Purpose	The current study aimed to explore the perceptions of school stakeholders on their responsibilities towards cybersafety and to propose a cybersafety community of purpose to mitigate cybersafety challenges in marginalised schools.
Background	The COVID-19 pandemic accelerated the adoption of information and communication technologies in education. In the post-pandemic era, schools are increasingly using technologies in curriculum delivery, data management, and communication. The increased access to cyberspace, however, exposes schools to cyber risks and cyberattacks.
Methodology	The study employed a qualitative exploratory methodology using case studies of four marginalised schools located in the Western Cape and Limpopo provinces of South Africa. We collected the data via semi-structured interviews of thirty participants who were stakeholders in a school context, including learners, educators, social workers, parents, and community leaders. Data analysis was based on an inductive approach with themes derived from data and the literature review.
Contribution	Using the social-ecological framework, the study showed that effective cybersafety is an ecological phenomenon that requires the understanding and involvement of individuals, the family of learners, and the school, in a community context. The study contributes to the body of knowledge by suggesting a bottom-up cybersafety community of purpose activity system for marginalised

Accepting Editor Dale Trott │ Received: April 30, 2025│ Revised: July 22, July 29, August 9, 2025 │ Accepted: August 20, 2025.

Cite as: Magunje, C., Chigona, W., & Makofane, B. I. (2025). Towards a Cybersafety Community of Purpose in Marginalised Schools. *Interdisciplinary Journal of Information, Knowledge, and Management, 20,* Article 27. https://doi.org/10.28945/5610

schools. Such a cybersafety community of purpose activity system would allow stakeholders to work together to gather resources and acquire actions that would lead to a cybersafe and cyber resilient school environment as an outcome. The activity system highlights the interrelationships between school stakeholders as they use cyberspace and how they can achieve the required outcomes, the family of learners, and the school, in a community context.

Finding

The findings of the study indicate that there is a disconnection in terms of cybersafety among school stakeholders in marginalised schools. There is a lack of clarity among stakeholders in terms of who is responsible for cybersecurity in the school context.

Recommendations for Practitioners

We propose that a bottom-up cybersafety community of purpose within an activity system would be an effective way to ensure the safety of school stakeholders as they use cyberspace.

Recommendations for Researchers

Researchers should implement the cybersafety community of purpose activity system in marginalised schools to determine its effectiveness.

Impact on Society

A cybersafety community of purpose would bring together all stakeholders within a school context, leading to effective cybersafety initiatives for a positive cybersecurity culture and cyber resilience within a school context.

Future Research

Future studies should adopt a design science approach to create and implement the cybersafety community of purpose activity system to determine its effectiveness.

Keywords

cybersecurity, cybersafety in education, community of purpose, marginalised schools

INTRODUCTION

The digital age has led to an increasing number of activities in different aspects of life being moved to cyberspace. In the education sector, the use of information communication technologies (ICTs) was accelerated by the COVID-19 pandemic, which led to the digitisation of most processes in the school, including curriculum delivery, data management, and administrative tasks (Torres & Thompson, 2020). In the digital age, schools have become caretakers of large data sets that include personal information, such as parents, learners, and educators (Richardson et al., 2020). Further, a growing number of learners are using digital devices to access cyberspace. All these highlight the importance of cybersecurity in schools (Kritzinger, 2020; Shambare et al., 2022).

South Africa is one of the most networked countries in sub-Saharan Africa, with a growing number of individuals who use online services (Mabece et al., 2017). As in most countries in sub-Saharan Africa, the pandemic increased the uptake of ICTs in schools. The increased dependence on the internet has become prominent in the social lives of stakeholders in school contexts. These stakeholders include parents, learners, educators, managers, administrative staff, and other entities in the community (Kritzinger, 2016). Cybercriminals, however, lurk in the virtual world to exploit the vulnerability of users to execute cyber harm. Unlike countries and corporate organisations, schools with limited financial resources might not be prepared to deal with cyber risks, leaving the various stakeholders in the school context vulnerable to cyberattacks (Magunje & Chigona, 2024a). In the South African context, marginalised schools are not adequately equipped to guarantee the cybersafety of their stakeholders since they operate under frugal conditions (Chigona et al., 2016).

We define marginalised schools as rural and low-income urban schools operating under constrained financial conditions with limited resources to meet all their needs and provide a wholesome learning experience for learners. These schools are inundated by several ICT-related challenges, including limited digital resources, cybersecurity and cybersafety knowledge and skills, and digital illiteracy among school stakeholders, leading to cybersecurity vulnerability (Magunje et al., 2024).

Cybersafety interventions within marginalised schools should focus on the empowerment of school stakeholders with a cybersecurity agency that leads to responsible online safety to achieve cybersafe school environments. Cyber resilience entails the ability and agility to withstand and overcome challenges that can be presented by the future of cybersecurity (Stuparu, 2020). Nations and corporate organisations encourage the formation of communities to share information across a region as they seek to ensure cybersafety and cyber resilience (Tagarev & Sharkov, 2016). The latter authors emphasise a holistic approach to cybersecurity and resilience of all interconnected segments that brings together various stakeholders (Shapira et al., 2021).

Disconnection among various stakeholders on cybersecurity within a school community exposes stakeholders to cyber threats and attacks. We postulate that marginalised schools can benefit from a community of purpose cybersafety activity system. By bringing stakeholders together, the cybersafety of everyone in a school community can be strengthened, particularly for the learner who can be the most vulnerable entity in a school context. Using the social-ecological framework, the current study mapped out the stakeholders within a school context and the community at large that influence and are influenced by cybersafety issues in a school (Bronfenbrenner & Morris, 1998).

A holistic approach to cybersafety interventions would address the issue of cybersafety through the cultivation of a cybersafety CoP – also within marginalised schools. A community of purpose (CoP) refers to a group of people who collaborate to support each other to achieve a common objective, often driven by a strong sense of shared values or vision (Stukes, 2016). A community of purpose is different from a community of practice. Unlike the latter, which entails a community of people with similar characteristics, the former is a heterogeneous group with a shared purpose. In this case, the shared purpose is the cybersafety of the school.

Through a CoP, various entities within the school community would be responsible for the communal cybersafety of the various school stakeholders. The success of a CoP would therefore be the effective involvement of all stakeholders towards cybersafety and cyber resilience in the school context. The current study thus sought to answer the following research questions:

1. What are the perceptions of school stakeholders of their responsibilities towards cybersafety?
2. How can a cybersafety community of purpose work to mitigate cybersafety challenges in schools?

Guided by the questions, the first objective of the current study was thus to explore the perceptions of school stakeholders of their responsibilities towards cybersafety within the school context. ‘Perceptions’ refer to an “individual’s construction of his or her reality, thus there is potential for perception to be affected by individuals’ self-concept” (Crandall et al., 2019, p. 75). Perceptions of school stakeholders, therefore, depend on their individual knowledge levels and personal experience with cybersafety-related issues (Maisikeli, 2020).

The second objective aimed to examine how a CoP within a school setting could help address cybersafety challenges. The study’s findings can assist ICT and education authorities in implementing cybersecurity measures in rural schools, fostering a culture of cybersafety and cyber resilience in marginalised communities. The study’s contribution could unite community members such as social workers, politicians, police, school officials, parents, and especially the learners, who are the most vulnerable in a school environment, to collectively fight cyberattacks. A cybersecurity CoP in marginalised schools would promote cybersecurity awareness among school stakeholders, which would, in turn, improve cybersafety for everyone in the community.

LITERATURE REVIEW

CYBERSECURITY AND CYBERSAFETY

Cybersecurity is crucial in ensuring the preservation of the availability of information integrity and confidentiality in cyberspace (Nam, 2019). The phenomenon has gained momentum in the digital age and the post-pandemic era, where the internet has become a critical resource in most aspects of life. Africa, like any other continent, is affected by many forms of cybercrime, which include cyberextortion, identity theft, social media scams, violation of privacy, hacking, phishing, and publishing illegal content (Eltahir & Ahmed, 2023; Marcum & Higgins, 2021). Cybersecurity is generally challenging in most organisations. When young people are involved, it becomes even more complex. The issue of online risks that may affect them should be taken into consideration, and counter-measures are needed to support young people and their guardians, such as parents, educators, and school managers, including the awareness that learners have of the various cyberthreats and risks (Quayyum et al., 2021).

Cybercriminals prey on the vulnerabilities and weaknesses of internet users with errors caused by people inevitably remaining high, thereby limiting risk mitigations (Richardson et al., 2020). When internet users practice poor cyber hygiene within school contexts, it compromises the users and gives cybercriminals unauthorised access to school data or personal information (Williams & Joinson, 2020). In the South African context, the school curriculum does not explicitly provide for cybersecurity education. There is, therefore, limited availability of cybersafety awareness and supporting material, resulting in a lack of knowledge and skills regarding cybersafety in marginalised schools (Kritzinger, 2016). Nonetheless, the increase in cyberattacks among users in marginalised schools cannot be underestimated, as studies have shown that stakeholders often fall victim to cybercrimes that include phishing, extortion, sextortion, and cyberbullying (Magunje et al., 2024; Magunje & Chigona, 2024b).

Without cybersafety awareness, internet users become the greatest threat to cybersecurity in an organisation. In a school context, cybersafety is compounded by the disparate populations within their contexts that are associated with misuse of computer resources (Aliyu et al., 2010). When stakeholders in school contexts are ignorant of cyber risks and continue to use digital technologies for educational and personal purposes with potentially irresponsible behaviour, they increase the surface attack for cybercriminals (Ulven & Wangen, 2021). In this sense, surface attacks refer to the gap within an institution, such as a school's security, which cybercriminals could compromise, and these are the exposed areas of a school that make the ICTs vulnerable to attacks (Giannakas et al., 2023). Mitigating vulnerabilities is a key factor in improving safety at both individual and institutional levels within a school setting.

Cybersecurity awareness is described as the level of users' understanding of the importance of information security and their responsibility to exercise sufficient information control over their data and the data and networks of the institution (Alshaikh et al., 2019). An individual's behaviour is determined by their knowledge and comprehension of cybersafety, including their beliefs, attitudes, perceptions, and experiences (Bada et al., 2015). The faulty or uneducated way a user responds to an ongoing cyberattack can be a vulnerability, which may lead to further repercussions (Nam, 2019).

Within a school context, learners are especially vulnerable. They require significant support due to their developing cognitive and social skills. They are at a stage of development where they are starting to test boundaries while lacking self-regulation skills (Pramod & Raman, 2014). With cybersafety knowledge and skills, learners can develop agency and adopt sustainable, secure online safety behaviours to participate more confidently in cyberspace (Renaud & Prior, 2021).

Marginalised schools in South Africa

In South Africa, schools are classified into quintiles as determined by the Department of Basic Education (van Dyk & White, 2019), which reflects whether a school is situated in a marginalised or affluent area. Schools are therefore classified into five categories, with Quintile 1 representing the poorest school and Quintile 5 the least poor. Government financial support is allocated based on the quintiles, as Quantile 1 to Quantile 3 schools do not pay fees. The financial support per learner is allocated on a sliding scale, with Quantile 1 receiving the highest allocation. All schools used in the current study fell under Quintiles 1 and 2 and were no-fee schools.

During the apartheid period in South Africa (1948-1994), black settlements known as townships were institutionalised communities based on racial discrimination associated with migrant labour. The apartheid legacy has also led to the sprawling informal settlements in metropolitan areas in South Africa over the past 25 years (Burger et al., 2017). In democratic South Africa, both townships and informal settlements are associated with high population densities. In these settlements, high unemployment rates and incremental rates of substance abuse and crime are common social ills (Chikoto, 2009). Similarly, rural areas are generally remote and relatively underdeveloped. Many schools, therefore, lack the necessary physical resources and basic infrastructure for sanitation, water, roads, transport, electricity, and ICTs (du Plessis & Mestry, 2019)

The use of mobile phones in South Africa has increased considerably, which has driven internet penetration levels high (Mojapelo, 2020). South Africa is one of the most connected countries in Africa. Connectivity has, however, led to a large number of cybercrime victims (Snail ka Mtuze & Musoni, 2023). An increase in cyber incidents, such as accidental data exposure or compromised websites, shows that South Africans are inexperienced and lack technical alertness when operating in cyberspace (Potgieter, 2019).

Data management is especially critical in South African schools, as the Department of Basic Education has implemented the South African School Administration Management System (SA-SAMS) for data management in all schools in the country (Magunje & Chigona, 2024a). Further to this positive development, various stakeholders in a school context derive benefits from cyberspace, including teaching and learning, administrative tasks, socialisation, and entertainment (Kritzinger, 2020). The increase in cyberattacks in educational institutions due to the large amount of personal information that these institutions hold has, however, highlighted the need for an increased culture of cybersecurity in schools (Chen & Shen, 2020). Further to the need to protect the systems and data of a school, stakeholders must be protected from cyber threats as they use cyberspace, more so learners, as they are the most vulnerable entity in a school context (Magunje et al., 2024).

Children's online safety has become a global issue that has attained international attention. The United Nations Children's Fund (UNICEF) has sought to protect children from emerging risks in cyberspace by promoting legal and policy reforms that align with international human rights (Andrews et al., 2020). Both primary and secondary school learners may be exposed to cyberthreats and can be susceptible to threats that include cyberbullying, exposure to inappropriate content, and accidental sharing of personal information (Cilliers & Chinyamurindi, 2020). In addition to cyberbullying, learners may be increasingly susceptible to phishing scams, hacking attempts, and online predators seeking personal information.

Because secondary school learners are more active on social media platforms, they are more vulnerable to these kinds of cyber threats as well as other forms of harassment (Farhangpour et al., 2019). Marginalised schools in South Africa face a myriad of cyberspace-related challenges, such as cyberbullying, online fraud, and phishing attacks among school stakeholders (Magunje & Chigona, 2024b). It is worth mentioning the important role of parents in the cybersafety of their children. To provide effective guidance as their children use the internet, parents need to be educated and well-informed about cybersafety themselves (Paraiso, 2019). Parents face the challenge of adapting to fast-advancing technology, while children tend to be dependent on internet services, particularly for entertainment activities (Crawford, 2013). Cybersafety knowledge is of paramount importance, as parents who are knowledgeable about cybersecurity are confident in ensuring and managing their children's use of technology (Giannakas et al., 2023; Zwilling et al., 2022).

Strategies to counteract the cyberthreats against stakeholders in school contexts are, therefore, a necessity (Kritzinger, 2016, 2020). The role of learners, parents, educators, and management, as well as other important entities within the community, cannot be underestimated if cybersafety is to be a priority in schools. The management of a school in the South African context is shared by the school management teams (SMTs) comprising the principal, deputy principal(s), and head of departments (Madimetsa & Saltiel, 2021). The SMTs work closely with the school governing body (SGB), comprising parents and learners, promoting their participation in school governance (Mncube, 2009). The role of SGBs in South African schools is to work closely with SMTs to implement educational policies (King & Mestry, 2023). In the absence of cybersecurity and cybersafety policies in schools, coupled with the limited cybersafety knowledge and skills, marginalised schools, however, face challenges when dealing with cybersecurity and cybersafety issues (Magunje et al., 2024; Magunje & Chigona, 2024a). We argue, therefore, that cybersafety resilience and culture can be achieved in marginalised schools when various stakeholders in a community create a cybersafety CoP.

SOCIAL-ECOLOGICAL FRAMEWORK

To map out and identify the stakeholders in a school context, we used the social-ecological framework (Sudbery & Whittaker, 2018). According to the framework, there is reciprocity between the environments and the individuals who live in them, and the interactions entail that one's environment influences them, and the environment is influenced by the individual (Salihu et al., 2015). We argue that effective cybersafety is an ecological phenomenon that requires the understanding and involvement of individuals, families, and the school in a community context. Through the social-ecological framework, a cybersafety culture within a school context is viewed as something that is not a straightforward outcome of individual behaviours. Instead, cybersafety behaviour and culture arise because of the complex interactions between individuals and the contexts within which they live (Espelage et al., 2018).

The social-ecological theory of development highlights the overlapping systems of the framework that illustrate the potential influence of both immediate and indirect factors on human behaviour (Cross et al., 2015). In line with the ecological framework, we drew a sample of respondents from different stakeholders affected by the cybersafety of the schools, particularly learners, as they are the most vulnerable. The sample for the study, as shown in Figure 1, comprised:

- School level (microsystem): educators, life orientation teachers, school counsellors (where available), learners, and school management.
- Community level (mesosystem): parents and guardians, social workers, law enforcement.
- Provincial education level (exo- and macrosystem): officers responsible for ICTs in schools, officers responsible for the safety and security in the schools, social workers, and community and religious leaders.

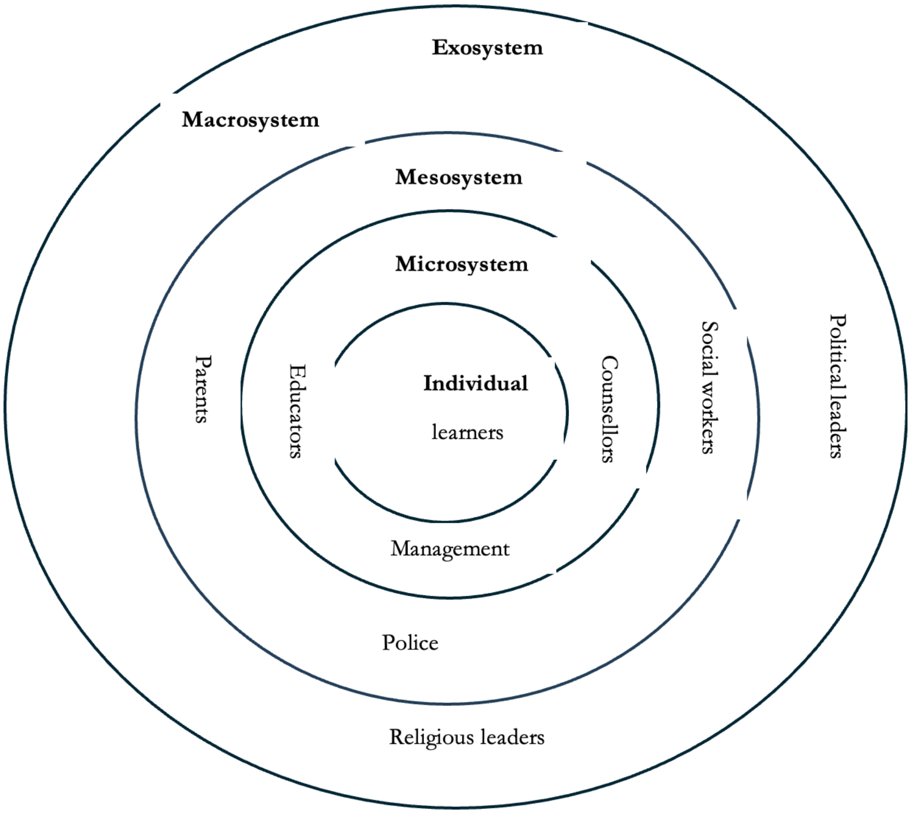

Figure 1. An adapted illustrated model of Bronfenbrenner and Morris' (1998) ecological framework for a school context

Community of Purpose

Communities of practice are commonly known to enact their purpose through grassroots efforts and social movements (Stukes, 2016). 'Communities of practice' is a well-known concept. It involves a group of people who voluntarily come together because they share a common concern or a passion, to explore these concerns and ideas, and to grow their practice (Lave & Wenger, 2001). Communities of practice are different from communities of purpose (CoPs), as CoPs develop because of a sense of community and a feeling that members belong and that they matter to one another and the group. They have a shared faith that members' needs will be met through their commitment to each other (Pakenham-Walsh, 2007). In the context of this study, the stakeholders identified in the social-ecological framework within a school context would come together to form a cybersafety CoP. Previous studies have shown an individualistic and a silo approach toward cybersecurity and cybersafety in marginalised schools that does not produce positive results in the school (Magunje et al., 2024; Magunje & Chigona, 2024b).

A CoP draws on stakeholders' virtues, such as a sense of engagement and responsibility for what they are doing and the way it is done in the cybersecurity of the school context (Warren, 1999). This allows stakeholders to come together to share what they know or to provide a social context of such knowledge, and to learn from each other regarding an aspect of their life, in this case, cybersafety (Stukes, 2016). A CoP creates a 'space' for stakeholders with various interests and functional silos to collaborate on achieving a common objective (Broganza, 2009). The fundamentals of a CoP are the influence that is derived from such a group, which is on such tangible and intangible resources as shared trust, adherence to group norms, and sanctions (Mahmood, 2015). A CoP would thus bring various stakeholders in marginalised schools together to contribute actively and constructively to cybersafety, thereby enhancing the online safety capabilities of a school community.

In most cases, CoPs take the form of a community of practices. The benefits of CoPs can be found in various communities, such as volunteer groups, religious communities, sports teams, and online forums (Alexander & Peñalver, 2008). An example would be a professional CoP where a group of people within a niche industry come together to learn from and support each other, and to contribute to the overall body of knowledge (Stanca et al., 2022). A cybersafety CoP within a school community would therefore lead to more engagement as various stakeholders come together.

METHODOLOGY

We adopted a multi-case study approach of four marginalised schools in two different provinces in South Africa, the Western Cape and Limpopo. The provinces were chosen specifically to represent an affluent province and an economically disadvantaged province, respectively. Using the interpretive approach, we appreciated and understood the thought process of various stakeholders as they dealt with cybersafety within a school context (Hollweck, 2016). We used purposive sampling, where the schools used in the study were from rural and low-income high-density urban areas. We purposely selected stakeholders within a school community who worked within the school sphere that was affected by cybersafety within the school (Yin, 2014). We held semi-structured interviews with various respondents in a school community, including learners, school managers, educators, parents, law enforcement officers, social workers, political leaders, and diverse community leaders. The interviews allowed a deep exploration of respondents' lived experiences as they faced cybersafety and cybersecurity in their daily lives. The qualitative study involved thirty respondents from the four case studies who were identified using the adapted social-ecological framework.

We adopted an inductive approach, which allowed us to interpret the data from the respondents' real-life experiences. The study led to contextual insights from stakeholders in a school community. Data was therefore analysed based on themes derived from the data. We used NVivo 14 data analysis software, which enabled the capturing and storing of all data material in a single repository. NVivo 14 further allowed easy navigation between different documents as well as the creation of codes assigned to the text, leading to easy visualisation of concepts arising from the data to give it meaning (Fereday & Muir-Cochrane, 2006).

The researchers followed the ethical protocols of their institutions when conducting research involving human subjects. We ensured that the research process did not cause harm to the research participants and protected their dignity. Confidentiality and anonymity of the respondents were maintained by assigning pseudonyms to the four schools used in the study. Western Cape schools are identified as WC1 and WC2, and Limpopo schools are identified as LMP1 and LMP2. The respondents are identified by a code and a serial number, which represents their school, i.e., LMP1C.

CASE DESCRIPTION

In the Western Cape, WC1 was a school in a high-density suburb, where an informal settlement was also developing at an alarming rate adjacent to the township. The community reflected high rates of poverty, unemployment, crime, and substance abuse. WC2 was in a commercial farming area, and the school catered to the farm laborers in the community. As in the case of WC1, the social ills of the community included high rates of unemployment, poverty, and substance abuse, as well as illiteracy.

In Limpopo, LMP1 was a low-income, high-density suburb with high rates of crime, unemployment, substance abuse, and poverty prevalent in the community. LMP2 is a rural school located in a subsistence farming area with challenges that include high rates of unemployment, illiteracy, and poverty.

FINDINGS

DIFFERENT VIEWS ON THE RESPONSIBILITY OF CYBERSAFETY IN SCHOOLS

There were different views on who was responsible for cybersafety within the school and the community. A learner expected educators to assist them with cybersafety-related issues. "When I got into an argument with someone here at school, they took it to social media; they were mocking me and harassing me online, so I reported it to one of the educators" (LMP1C).

Parents also felt that educators were responsible for cybersafety. "It is the teacher's responsibility. Not everyone else involved may be so enlightened with information on what to do online, so we should ask the teachers" (WC1D). Due to their role of imparting knowledge, the rationale here is that educators should be responsible for sharing cybersafety knowledge within the school. Other stakeholders in the community also expected educators to be actively involved in cybersafety in schools.

> Educators must talk about cybersafety. They should talk to learners about this each week to provide learners with guidance. (LMPIA, community sports coordinator)

Some educators felt that school management, as leaders of the school, were responsible for cybersafety in the school:

> When kids face problems or are attacked online, I just tell them to take it to the principal. (WC2C)
>
> If we face any problems with cybersafety for learners, even among us, we tell the principal, because as principals, they have policies. (LMP1A)

Other community stakeholders also believed cybersafety-related issues should be handled by the principal.

> I have dealt with cases of learners bullying each other online. I tried to stop them, and I spoke to the principal and sent him messages so he could deal with it. (LMP2A, ward committee member)
>
> We must talk to the principal so that he changes his policies so that they can include cybersecurity and cybersafety. (LMP2D, community circuit leader)

On their side, school managers, however, felt, "cybersecurity was not one of the school's priorities" (WC2A). Further, management had inadequacies when it came to cybersafety. For example, a school manager highlighted that they had "no policy on cybersecurity and cybersafety at our school for victims or what to do" (WC2E).

A member of the SGB, however, believed all cybersafety should be handled by "when we have a cybersafety problem, we should go to a school social worker" (WC2D). This perception was shared by a stakeholder who perceived that it is the role of the school to upgrade, because it is still ignorant of cybersafety issues. "I would appreciate it if they pulled up their socks" (LMP1F, royal council member). In the South African context, "royal council" refers to the structures within traditional leadership systems often found in rural areas. The councils are responsible for cultural preservation and community affairs within ethnic groups (Ntlama-Makhanya, 2024).

CYBERSAFETY RESPONSIBILITIES SHIFTED TO PARENTS

Stakeholders within the school community regarded the role of parents as central to cybersafety in schools. A learner remarked, "As teenagers, we cannot deal with certain issues on the internet … I think parents should not allow us to bring phones to school because of cybercrime." (WC1B)

A school manager highlighted:

> The government in South Africa has brought the parents closer to school to the extent that they are defending the school in terms of being robbed and being burnt, so they can assist in cybersafety, as they are defending the school. (WC1B)

Parents were, however, not seen to be performing this duty effectively. Other stakeholders felt they failed to do this due to negligence when it comes to learners' cybersafety. It was noted that some "parents tend to look away from this cyber thing, they don't pay too much attention." (LMP2C). Another reason why parents failed to perform this duty was low literacy levels. This is specifically so, since these parents lived in marginalised communities.

> Most of our parents are in the township; they're not literate, and they have difficulty working with the internet and safety. (WC1D, educator)

> Parents don't even know how to work with a cell phone or even with a computer, and they are ill-equipped to assist with cybersafety, but children are the cleverest with digital things. (WC2H, police officer)

On the increasing rate of online fraud and phishing in the community, a political counsellor highlighted "the need to invite banks to come and make parents aware of these things" (LMP1E).

Cybersecurity is Assigned to Law Enforcement Agencies

Law enforcement agencies – police officers in the context of this study – play a crucial role in ensuring the physical safety and security of community members in any community setting (Jennings & Perez, 2020). School stakeholders, therefore, assigned the responsibility of cybersafety to the police.

> The police must come talk to us and bring us up to date on what and how to go about online safety. (LMP1G, educator)

> The police must help us understand this cybersafety thing. (WC1F, parent)

> Maybe a police officer can bring the community together and talk about cybersafety. (WC2F, member of the general school board)

Some stakeholders, however, felt that law enforcement was not capacitated to handle cybersafety issues adequately.

> If you go to the police [station], sometimes the police don't even serve our people. They confuse us on cybersecurity. (LMP2E, politician)

> They [the police] don't offer much assistance. They just advise us to be more careful. (LMP2F, church pastor)

One reason that was cited for no or wrong actions by law enforcement agencies was a lack of appropriate knowledge and skills on cybersafety. A police officer confirmed that they were not equipped to deal with cybersecurity in school:

> We are just trying; we do not have enough knowledge on cybersecurity in the community. We take such issues back to the principal and then maybe send e-mails to the education department. It is very difficult. (WC2I, police officer)

Police respondents were aware of their limited cybersafety knowledge. They believed that cybersecurity specialists should assist them. "I think that professionals in the field of cybersecurity should assist us on how to best handle cybersecurity and cybersafety issues that may arise in the community" (LMP1H).

Discussion

Confusion on Responsibility

The findings highlight that there was no clarity on who was responsible for cybersafety in a school context. Different stakeholders assigned the responsibility to someone else, and nobody felt they were responsible. There were, however, sentiments from a respondent that cybersafety within the school context should be a concerted effort amongst different stakeholders: "… we must form a forum, between some churches, the school, and organisations in the community to make community members aware of cybersafety … we must ask the police to assist us with that" (LMP2F).

The findings indicate that school stakeholders are overwhelmed with cybersafety within their communities. Whilst parents and community members have high expectations of the role of the school in cybersecurity and cybersafety, neither school management nor educators see these important issues as their responsibility. This might be because both these entities have limited knowledge and skills on the phenomenon.

The current study found a perception among school stakeholders that parents should take additional cybersafety responsibilities for learners. While such a situation would be ideal, the findings show that marginalised schools are inundated with many challenges that include both general illiteracy and digital illiteracy among parents, which render them powerless on cybersafety-related issues.

The need to capacitate police officers with cybersecurity and cybersafety knowledge is paramount in marginalised schools, as respondents felt helpless in the face of cybersafety and cybersecurity-related issues in their contexts.

> To be honest with you, I am not familiar with this cybersafety. I still need to learn about it. I know that in our department, there's a component that deals with it. Getting training is the only way that we can protect the security of an individual or a school." (LMP2H, police officer)

Law enforcement agencies – in this case, police officers – are crucial within any community, as they are mandated to keep the community safe. Nonetheless, the findings indicate that school stakeholders in a community setup expect the police to protect them from cyberattacks. Participating police officers were, however, not equipped to assist with cybersecurity-related issues. Other stakeholders within the adapted social-ecological framework were also ineffective when dealing with cybersafety; instead of coming together to deal with cybersafety, stakeholders, however, assigned responsibility to one stakeholder or another.

The Cybersafety Community of Purpose Modus Operandi

The findings highlight the lack of clarity of who is responsible for cybersafety in a school context, including the need for capacitation with cybersafety knowledge and skills for all stakeholders in a school community. As suggested by a respondent, "the authorities must call the parents of all learners to the community hall to inform them and let them know about cybersafety so that they can educate or teach each other and their children how to behave online" (LMP2G).

The responsibility for cybersafety should be shared. We are therefore proposing that a cybersafety CoP activity system would be effective in dealing with online safety in a school context. Instead of working in silos and assigning blame to each other, a cybersafety CoP within marginalised schools would allow stakeholders to be each other's keeper when it comes to cyberattacks. Together, members of the CoP would work to gather resources, including experts who would provide the required cybersecurity, knowledge, skills, and awareness for the whole community.

Membership of the CoP would be based on the social-ecological system of a school (Cross et al., 2015). Following the mapping of the social-ecological theory, the findings of the current study showed the varied members of the community who form part of the school, as shown in Figure 2.

Members of the CoP could include social workers, church leaders, politicians, the police, school authorities, parents, and especially the learner, who is the most vulnerable entity in a school context. A cybersecurity CoP in marginalised schools would lead to a cybersecurity agency among school stakeholders that would enhance the cybersafety of all stakeholders in the community.

Cybersafety knowledge and skills, which can be acquired through training and awareness campaigns, are crucial for all stakeholders in marginalised schools. It is, therefore, imperative that stakeholders come together to acknowledge their cybersafety-related challenges and inadequacies and forge the way forward. Most interventions within marginalised contexts tend to be imposed on communities through a top-down approach. Such approaches fail to include the community meaningfully in the design of the solution (Lorini et al., 2019). We are proposing a bottom-up approach towards the development of initiatives that would address cybersafety within marginalised schools. The collective nature of a CoP would empower the stakeholders to have agency to contribute to possible cybersafety solutions.

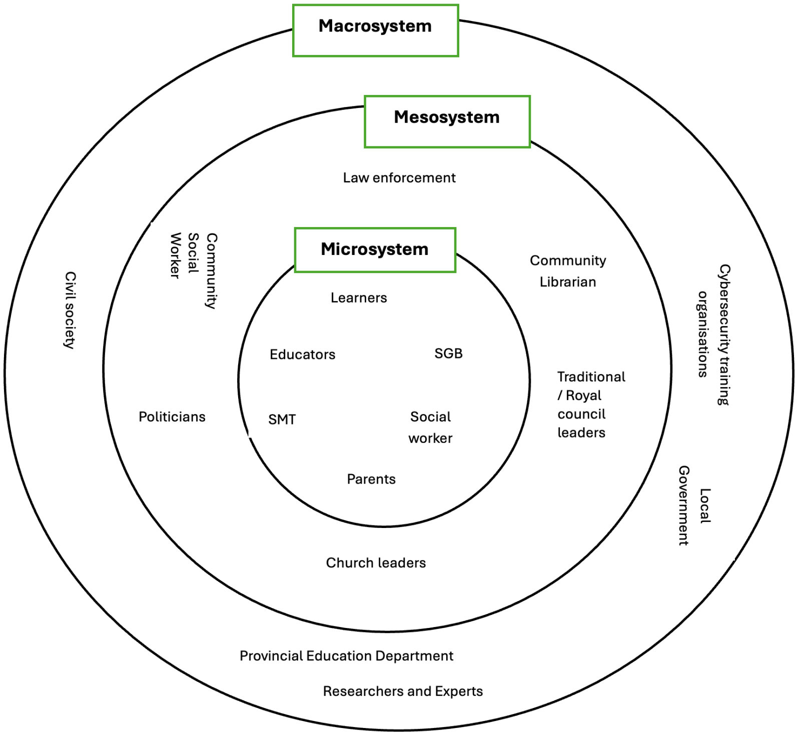

Figure 2. Representation of a cybersafety community of purpose

Learners should be part of the CoP, as they are the most vulnerable entity within a school community and should be most protected from cyber threats. The South African school system requires secondary schools to establish a representative council of learners, who also form part of the SGB (Hunt, 2014). Learner representatives should be part of the CoP in secondary schools because they are more mature than primary school learners and can make meaningful contributions. Representatives of the stakeholders in the microsystem – learners, educators, school management, members of the SGB, and selected parents – should be part of the CoP, as these would be the voice of the bodies they represent in the community. The composition of the CoP in the mesosystem would include the police because of their role as protectors in the community. Community social workers should be part of the mesosystem as they play an important role in the psychosocial status of the community.

There is, however, a need for flexibility among the other members of the CoP, depending on who is responsible for and committed to the safety and development of the school and the community. The involvement of community leaders in the CoP, such as political leaders, Royal Council members, and church pastors, may not be uniform in schools. Such leaders are crucial to the success of the cyber-safety CoP, as they play an innate role in the community, which is valuable to cybersafety because of their positioning in society, as they and their contribution are readily accepted. Further, these leaders have the respect and power to tap into resources needed to raise cybersecurity awareness from the macrosystem, which could work to the benefit of the school community.

COMMUNITY OF PURPOSE ACTIVITY SYSTEM

To address the role of the community in cybersafety and the need for agency among the various stakeholders in a school fully, the cybersafety CoP should have clear objectives, tools and instruments, rules, and clear roles assigned through division of labour. Without clear roles for each stakeholder in the community and without well-defined objectives and outcomes, the CoP might become less effective and redundant. We therefore propose a CoP activity system that can be presented through activity theory. Activity theory is a framework that considers individuals with shared needs or motives that drive an activity collectively (Leont'ev, 1981). Activity theory complements CoP in that this theory brings together people who have the same goal. The theory emphasises the interrelationship between the subjects (school stakeholders) and their community (school context) (Engeström, 1987). Figure 3 shows how the cybersafety CoP can be conceptualised in an activity system.

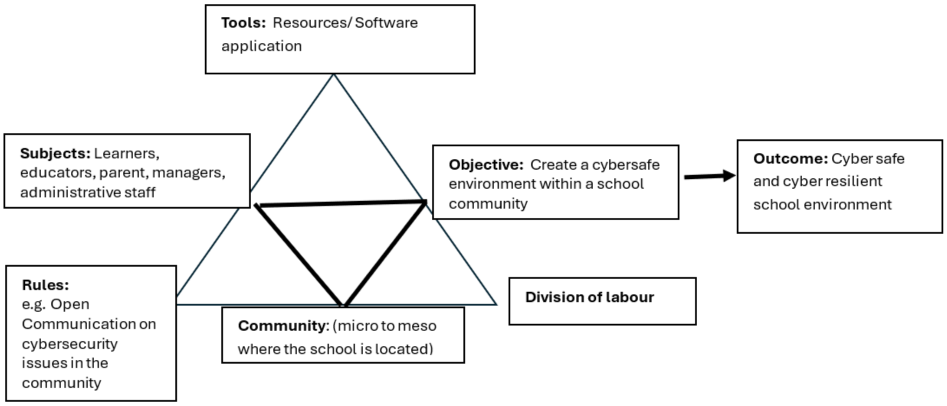
Tools: Resources/ Software application
Subjects: Learners, educators, parent, managers, administrative staff
Objective: Create a cybersafe environment within a school community
Outcome: Cyber safe and cyber resilient school environment
Rules: e.g. Open Communication on cybersecurity issues in the community
Community: (micro to meso where the school is located)
Division of labour

Figure 3. Cyber safety community of purpose activity system for marginalised schools

Activity theory highlights the interrelationships between learners, parents, educators, and school managers as they use cyberspace and the way they can achieve the activity systems outcome. Creating a cyber safety activity system allows for the determination of the goal or outcome within the school community. The outcome would be the creation of a cybersafe and cyber-resilient school environment. This outcome would be achieved through a clear objective of creating a cybersafe environment within a school community. Agency in AT is expressed through action as the basic unit of an activity, where activity is comprised of one or more actions which, when performed through the tools (in this case, cybersafety resources and a software application), achieve a conscious goal (Bedny & Karwowski, 2004). In the current study, the cybersafety activities of the members of the community would lead to the required outcome, which is acquiring a cybersafety agency by the subjects of the activity system, to practice cyber hygiene, which would enhance cybersafety in the community.

While resources might include cybersafety awareness campaigns and the use of cybersecurity resource people, a software application can be a readily available cybersafety tool for all stakeholders.

There have been notable upward trends in both internet and mobile phone penetration in South Africa (Independent Communications Authority of South Africa, 2025), which makes a cybersafety software application a viable option. It is noteworthy that, in 2022, the cellular population coverage in South Africa was for 3G, which was recorded at 100%, while 4G/LTE stood at over 98% (Ngwenya et al., 2023). Further, most marginalised communities in South Africa have free public Wi-Fi provided by the government; thus, using a software application that is widely accepted in a community might prove to be feasible, as there might not be challenges associated with the cost of data (Du Bois & Chigona, 2018). With a determined cybersafety CoP within their communities, a repository of cybersafety information might be useful for the whole community, which can be a software application as a tool in the activity system, such as a WhatsApp group or channel. We propose that the WhatsApp group should have artificial intelligence-enabled chatbots that can respond to cybersecurity and cybersafety queries. The artificial intelligence-enabled application would identify prompts from messages sent by stakeholders in the community and point them to relevant cybersafety resources or a recommended course of action to be safe online.

Rules are important in the CoP if the activity system is to be effective. The cybersafety CoP should have rules that govern the working of the CoP as well as that of the school community. Open communication within the community should be encouraged between all stakeholders, especially those within the micro- and mesosystems. Division of labour is important in the CoP, as it ensures responsibility and accountability for the cybersafety issue among the CoP and the stakeholders in the activity system. This would eradicate the issue of uncertainty on who should be responsible for cybersafety in the school, as highlighted in the findings. Through the concept of division of labour, AT highlights the role of context and the surrounding community in the process of transformation from individual action to collective activity, and exactly how the division of labour affects individual action in collective activity (Hardman, 2008). This would encourage dependence on each other and assist the community in realising their cybersafety shortcomings so they can seek external cybersafety experts and resources to fulfil their objectives where necessary. The prime unit of analysis in AT is the collective artefact-mediated and object-oriented activity system, as seen in its network relations with other systems (Engeström, 1987). By coming together as a group with one accord, the cybersafety CoP would work together in terms of the single-minded need to promote and enhance cybersafety in the school community, which would result in a cybersafe and cyber-resilient school environment.

CONCLUSION

Stakeholders in marginalised schools face a myriad of challenges as they operate with constrained resources. The current study highlighted that, despite the socio-economic statuses of Western Cape and Limpopo as affluent and disadvantaged provinces, respectively, the cybersecurity and cybersafety perspectives and disconnection among school stakeholders in marginalised schools are similar. In the digital age, the internet has brought many benefits in education, such as enhanced learning processes because of increased access to learning resources, improved communication with stakeholders, and data storage. The limited resources in marginalised schools, however, expose them to cyberattacks and risks, as they cannot afford to acquire cybersecurity knowledge or raise cybersecurity awareness initiatives for the various stakeholders of the school.

The study found that stakeholders in marginalised school contexts are overwhelmed by the cybersecurity challenges faced in the community. The absence of cybersafety knowledge and skills among all stakeholders, as well as the lack of responsibility among each of them in terms of cybersecurity-related issues, increases their vulnerability to cyberattacks. We conclude that a cybersafety CoP would bring together all stakeholders within a school context, leading to effective cybersafety initiatives for a positive cybersecurity culture within the school context. Further, we propose that a bottom-up cybersafety CoP within an activity system would be an effective way to ensure the safety of school stakeholders as they use cyberspace. The activity system allows stakeholders within a school context to emphasise the activities of each stakeholder, highlighting the responsibility of everyone in the community in terms of their role in ensuring a cybersafe school environment. Future studies should adopt a design science approach to develop and implement such a community of practice.

References

Alexander, G. S., & Peñalver, E. M. (2008). Properties of community. *Theoretical Inquiries in Law, 10*(1), 127-160. https://doi.org/10.2202/1565-3404.1211

Aliyu, M., Abdallah, N. A. O., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010, December). Computer security and ethics awareness among IIUM students: An empirical study. *Proceedings of the 3rd International Conference on Information and Communication Technology for the Moslem World, Jakarta, Indonesia,* A52-A56. https://doi.org/10.1109/ICT4M.2010.5971884

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019, June). Toward sustainable behaviour change: An approach for cyber security, education, training, and awareness. *Proceedings of the 27th European Conference on Information Systems, Stockholm & Uppsala, Sweden.*

Andrews, D., Alathur, S., & Chetty, N. (2020). International efforts for children online safety. *International Journal of Web-Based Communities, 16*(2), 123-133. https://doi.org/10.1504/IJWBC.2020.107146

Bada, M., Sasse, A., & Nurse, J. R. C. (2015, February). Cybersecurity awareness campaigns: Why they fail to change behavior. *Proceedings of the International Conference on Cyber Security for Sustainable Society, Coventry, UK,* 118-131.

Bedny, G. Z., & Karwowski, W. (2004). Activity theory as a basis for the study of work. *Ergonomics, 47*(2), 134-153. https://doi.org/10.1080/00140130310001617921

Broganza, A. (2009). Communities of purpose: Eliminating knowledge and enhancing practices in transformational government programmes. In V. Weerakkody, M. Janssen, & Y. Dwivedi (Eds.), *Handbook of research on ICT-enabled transformational government: A global perspective* (pp. 197-212). IGI Global. https://doi.org/10.4018/978-1-60566-390-6.ch011

Bronfenbrenner, U., & Morris, P. A. (1998). The ecology of developmental processes. In W. Damon & R. M. Lerner (Eds.), *Handbook of child psychology: Theoretical models of human development* (5th ed., pp. 993–1028). John Wiley & Sons.

Burger, R., van der Berg, S., van der Walt, S., & Yu, D. (2017). The long walk: Considering the enduring spatial and racial dimensions of deprivation two decades after the fall of apartheid. *Social Indicators Research, 130*, 1101-1123. https://doi.org/10.1007/s11205-016-1237-1

Chen, I. L., & Shen, L. (2020). The cyberethics, cybersafety, and cybersecurity at schools. In Information Resources Management Association (Ed.), *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1395-1412). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch082

Chigona, W., Mudavanhu, S. L., & Lwoga, T. (2016). Framing telecentres: Accounts of women in rural communities in South Africa and Tanzania. *CONF-IRM 201 Proceedings*. https://www.researchgate.net/publication/303843501_Framing_telecentres_Accounts_of_women_in_rural_communities_in_South_Africa_and_Tanzania

Chikoto, T. (2009). *Informal settlements in South Africa* [Bachelor Thesis, University of Pretoria].

Cilliers, L., & Chinyamurindi, W. (2020). Perceptions of cyberbullying 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. https://doi.org/10.1002/isd2.12131

Crandall, K. S., Noteboom, C., El-Gayar, O., & Crandall, K. (2019). High school students' perceptions of cybersecurity: An explanatory case study. *Issues in Information Systems, 20*(3), 74-82. https://doi.org/10.48009/3_iis_2019_74-82

Crawford, R. (2013). *The ICT teacher's handbook: Teaching, learning and managing ICT in the secondary school.* Routledge

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

Du Bois, J., & Chigona, W. (2018). Use of free public Wi-Fi and telecentres in disadvantaged communities in the Western Cape. *Development Informatics Association*, 2, 1-10.

du Plessis, P., & Mestry, R. (2019). Teachers for rural schools – A challenge for South Africa. *South African Journal of Education, 39,* Article 1774. https://doi.org/10.15700/saje.v39ns1a1774

Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Information Sciences Letters, 12*(1), 171-183. https://doi.org/10.18576/isl/120113

Engeström, Y. (1987). *Learning by expanding: An activity theoretical approach to developmental research.* Orienta-Konsultit.

Espelage, D. L., Hong, J. S., & Valido, A. (2018). Cyberbullying in the United States. In A. C. Baldry, C. Blaya & D. P. Farrington (Eds.), *International perspectives on cyberbullying: Prevalence, risk factors and interventions* (pp. 65-99). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-73263-3_4

Farhangpour, P., Maluleke, C., & Mutshaeni, H. N. (2019). Emotional and academic effects of cyberbullying on students in a rural high school in the Limpopo province, South Africa. S*outh African Journal of Information Management, 21(1),* a925. https://doi.org/10.4102/sajim.v21i1.925

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods, 5*(1), 80-92. https://doi.org/10.1177/160940690600500107

Giannakas, F., Troussas, C., Krouska, A., Voyiatzis, I., & Sgouropoulou, C. (2023). Blending cybersecurity education with IoT devices: A u-Learning scenario for introducing the man-in-the-middle attack. *Information Security Journal: A Global Perspective, 32(5),* 371-382. https://doi.org/10.1080/19393555.2022.2100297

Hardman, J. (2008). Researching pedagogy: An activity theory approach. *Journal of Education, 45*(1)*,* 65-95.

Hollweck, T. (2016). *Case study research design and methods* (5th ed.). Sage.

Hunt, F. (2014). Learner councils in South African schools: Adult involvement and learners' rights. *Education, Citizenship and Social Justice, 9*(3), 268-285. https://doi.org/10.1177/1746197914545928

Independent Communications Authority of South Africa. (2025, March 31). *The state of the ICT sector of South Africa.* https://www.icasa.org.za/uploads/files/The-State-of-the-ICT-Sector-Report-of-South-Africa-2025.pdf

Jennings, W. G., & Perez, N. M. (2020). The immediate impact of COVID-19 on law enforcement in the United States. *American Journal of Criminal Justice, 45*(4), 690-701. https://doi.org/10.1007/s12103-020-09536-2

King, J., & Mestry, R. (2023). The oversight functions of school governing bodies in the management of budgets. *Perspectives in Education, 41*(4), 177-193. https://doi.org/10.38140/pie.v41i4.7512

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

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

Lave, J., & Wenger, E. (2001). Legitimate peripheral participation in communities of practice. In J. Clarke, A. Hanson, R. Harrison, & F. Reeve (Eds.), *Supporting lifelong learning* (pp. 121-136). Routledge. https://doi.org/10.4324/9780203996287-11

Leont'ev, A. N. (1981). The problem of activity in psychology. In J. V. Wertsch (Ed.), *The concept of activity in Soviet psychology* (pp. 37-71). M. E. Sharpe.

Lorini, M. R., Densmore, M., Johnson, D., Hadzic, S., Mthoko, H., Manuel, G., Waries, M., & van Zyl, A. (2019). Localize-it: Co-designing a community-owned platform. In K. Krauss, M. Turpin, & F. Naude (Eds.), *Locally relevant ICT research* (pp. 243-257). Springer. https://doi.org/10.1007/978-3-030-11235-6_16

Mabece, T., Futcher, L., & Thomson, K.-L. (2017). South African computing educators' perspectives on information security behaviour. In M. Bishop, L. Futcher, N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education for a global digital society* (pp. 121-132). Springer. https://doi.org/10.1007/978-3-319-58553-6_11

Madimetsa, J. M., & Saltiel, K. C. M. (2021). Empowerment of the school management team by secondary schools' principals in Tshwane West District, South Africa. *Educational Research and Reviews, 16*(4), 93–103. https://doi.org/10.5897/err2020.4076

Magunje, C., Bagui, L., & Chigona, W. (2024). Educators' perspectives on cybersecurity: Case of resource-constrained schools in South Africa. In W. Chigona, S. Kabanda & L. F. Seymour (Eds.), *Implications of information and digital technologies for development* (pp. 91-103). Springer. https://doi.org/10.1007/978-3-031-66986-6_7

Magunje, C., & Chigona, W. (2024a). Educators' cybersecurity vulnerabilities in marginalised schools in South Africa. In A. Gerber (Ed.), *South African computer science and information systems research trends* (pp. 347-360). Springer. https://doi.org/10.1007/978-3-031-64881-6

Magunje, C., & Chigona, W. (2024b). Perceptions of school management on cyber threats: The case of resource-constrained schools in South Africa. In H. Twinomurinzi, N. K. Msweli, S. Gumbo, T. Mawela, E. Mtsweni, P. Mkhize & E. Mnkandla (Eds.), *EPiC Series in Education Science, 6*, 53-65. https://doi.org/10.29007/3542

Mahmood, K. (2015). Social capital: From concept to theory. *Pakistan Journal of Science, 67*(1).

Maisikeli, S. (2020, March). UAE cybersecurity perception and risk assessments compared to other developed nations. *Proceedings of the 3rd International Conference on Information and Computer Technologies, San Jose, CA, USA*, 432-439. https://doi.org/10.1109/ICICT50521.2020.00075

Marcum, C. D., & Higgins, G. E. (2021). A systematic review of cyberstalking victimization and offending behaviors. *American Journal of Criminal Justice, 46*(6), 882-910. https://doi.org/10.1007/s12103-021-09653-6

Mncube, V. (2009). Perceptions of the principal's role in democratic school governance in South Africa. *Journal of Educational Administration and History, 41*(1), 29-43. https://doi.org/10.1080/00220620802604594

Mojapelo, S. M. (2020). The internet access and use in public libraries in Limpopo Province, South Africa. *Public Library Quarterly, 39*(3), 265-282. https://doi.org/10.1080/01616846.2019.1622980

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society, 58*, 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Ngwenya, S. O., Heymann, R., Swart, T. G., & Lysko, A. A. (2023). A comparative analysis of urban and rural broadband penetration and access trends in South Africa. In P. Kommers, M. Macedo, G. C. Peng, A. Abraham, & L. Rodrigues (Eds.), *Proceedings of the International Conferences on ICT, Society, and Human Beings* (pp. 64-72). IADIS Press.

Ntlama-Makhanya, N. (2024). The role of the royal family in transforming the institution of traditional leadership in South Africa. *Journal of Law, Society and Development, 11*, 1-20. https://doi.org/10.25159/2520-9515/15117

Pakenham-Walsh, N. (2007). 'Healthcare information for all by 2015': A community of purpose facilitated by Reader-Focused Moderation. *Knowledge Management for Development Journal, 3*(1), 93-108. https://www.km4djournal.org/index.php/km4dj/article/view/96/156

Paraiso, E. L. (2019). *Towards a cyber safety information framework for South African parents* [MIT Dissertation, University of Pretoria, Pretoria, South Africa].

Potgieter, P. (2019). The awareness behaviour of students on cyber security awareness by using social media platforms: A case study at Central University of Technology. In K. Njenga (Ed.), *Proceedings of the 4th International Conference on the Internet, Cyber Security and Information Systems* (pp. 272-280). EasyChair. https://doi.org/10.29007/gprf

Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research, 9*(23), 19133-19144.

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Renaud, K., & Prior, S. (2021). The "three M's" counter-measures to children's risky online behaviors: Mentor, mitigate and monitor. *Information and Computer Security, 29*(3), 526-557.

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.

Salihu, H. M., Wilson, R. E., King, L. M., Marty, P. J., & Whiteman, V. E. (2015). Socio-ecological model as a framework for overcoming barriers and challenges in randomized control trials in minority and underserved communities. *International Journal of Maternal and Child Health and AIDS, 3*(1), 85-95. https://doi.org/10.21106/ijma.42

Shambare, B., Simuja, C., & Olayinka, T. A. (2022). Educational technologies as pedagogical tools: Perspectives from teachers in rural marginalised secondary schools in South Africa. I*nternational Journal of Information and Communication Technology Education, 18*(1), 1-15. https://doi.org/10.4018/ijicte.307109

Shapira, N., Ayalon, O., Ostfeld, A., Farber, Y., & Housh, M. (2021). Cybersecurity in water sector: Stakeholders' perspective. *Journal of Water Resources Planning and Management, 147*(8). https://doi.org/10.1061/(asce)wr . 1943-5452.0001400

Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review, 4*(3), 299-323. https://doi.org/10.1365/s43439-023-00089-8

Stanca, L., Dabija, D. C., & Păcurar, E. (2022). Community of practice: Converting IT graduate students into specialists via professional knowledge sharing. *Kybernetes, 51*(2), 557-581. https://doi.org/10.1108/K-10-2020-0711

Stukes, F. (2016). *Communities of purpose* [Doctoral dissertation, University of North Carolina at Charlotte]

Stuparu, A. A. (2020). *Educational pathways to national cyber resilience: The Australian story* [Doctoral dissertation, Australian National University].

Sudbery, J., & Whittaker, A. (2018). Bronfenbrenner's ecological model. Human growth and development (pp. 287-290). Routledge. https://doi.org/10.4324/9780203730386-13

Tagarev, T., & Sharkov, G. (2016). Multi-stakeholder Approach to Cybersecurity and Resilience. *Information & Security: An International Journal, 34(1),* 59-68. https://it4sec.org/system/files/3405_multi-stakeholder_cybersecurity.pdf

Torres, M., & Thompson, N. (2020). Toward a cybersecurity adoption framework for primary and secondary education providers. *ACIS 2020 Proceedings*. https://aisel.aisnet.org/acis2020/93/

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39. https://doi.org/10.3390/fi13020039

van Dyk, H., & White, C. J. (2019). Theory and practice of the quintile ranking of schools in South Africa: A financial management perspective. *South African Journal of Education, 39*, Article 1820. https://doi.org/10.15700/saje.v39ns1a1820

Warren, R. C. (1999). Empowerment in a community of purpose. In J. J. Quinn & P. W. F. Davies (Eds.), *Ethics and empowerment* (pp. 369-392). Palgrave Macmillan. https://doi.org/10.1057/9780230372726_14

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity, 6*(1), 1-16. https://doi.org/10.1093/cybsec/tyaa001

Yin, R. K. (2014). *Case study research design and methods* (5th ed.). Sage.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cybersecurity awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1)*,* 82-97. https://doi.org/10.1080/08874417.2020.1712269

AUTHORS

Caroline Magunje, PhD, is a Senior Researcher and the lead researcher of Cybersecurity for Schools at Cybersecurity Capacity Centre for Southern Africa (C3SA), University of Cape Town. Her research focuses on e-Learning, Cybersecurity in Education, Gender, ICTs, and ICT for human development.

Wallace Chigona is a Professor of Information Systems at the University of Cape Town, South Africa. He is currently the Director of the Cybersecurity Capacity Centre for Southern Africa (C3SA). His research focuses on Information and Communication Technologies (ICT) policies and the use of ICTs for human development. He has researched how disadvantaged communities in different African countries use and are affected by ICTs.

Inneth Baby Makofane, PhD, is an emerging scholar in the field of education with a strong academic and professional background. She is currently serving as a Post-Doctoral Research Fellow at the University of Limpopo. Her research interests span teaching and learning, evaluation of teaching, curriculum development, assessment, teacher development, and inclusive education across both basic and higher education contexts.