EPiC Series in Education Science

Volume 6, 2024, Pages 53–65

Proceedings of the NEMISA Digital Skills Summit and Colloquium 2024

Perceptions of school management on cyber threats: The case of resource-constrained schools in South Africa

Caroline Magunje and Wallace Chigona
University of Cape Town, Cape town South Africa.
caroline.magunje@uct.ac.za, wallace.chigona@uvr.ac.za

Abstract

Globally, most countries are realising the importance of cybersecurity in all aspects of life including education. Most African countries, however, have not prioritised cybersecurity especially in education despite the high levels of cyber-criminal activities on the continent. The integration of information communication technologies in curriculum delivery, data management and administrative tasks calls for cybersecurity diligence within a school system. School management, as custodians of various school stakeholders in their administrative and pastoral care responsibilities, have a responsibility towards cybersecurity in schools. Cyber-threats and risks can disrupt regular school operations, negatively affecting the security of learners, educators, administrative staff, parents, and the community at large. Resource-constrained schools can be particularly vulnerable as they generally operate under frugal conditions. There is, however, a paucity of cybersecurity for school leadership in literature. This study, therefore, attempts to answer the question: What are the perceptions of cyber threats among school management in resource-constrained schools? The study employed a qualitative exploratory case study methodology. We collected the data through semi-structured interviews from four schools in the Western Cape and Limpopo provinces. These represent an affluent and a rural province. The data was analysed using thematic analysis based on the Capability Approach. Findings suggest that school managers cybersecurity self-efficacy is low, and their limited cybersecurity knowledge deprives the cybersecurity capabilities of the various stakeholders under their leadership. Their environment does not provide cybersecurity capacity building to boost their confidence as they deal with and address various cybersecurity related matters in their context. The study contributes to cybersecurity in education by highlighting the cybersecurity perceptions of school managers in resource-constrained schools. These findings will pavethe way for initiatives that capacitate cybersecurity knowledge and skills among school managers and cultivate a culture of cyber safety in schools.

H. Twinomurinzi, N.T. Msweli, S. Gumbo, T. Mawela, E. Mtsweni, P. Mkhize and E. Mnkandla (eds.),
NEMISA DigitalSkills 2024 (EPiC Series in Education Science, vol. 6), pp. 53–65

1 Introduction

Information communication technologies (ICTs) have become ubiquitous in the 21st century embedding themselves in most facets of life, including education. Globally schools have embraced the use of technology in teaching and learning, administrative tasks, and community engagement (Torres & Thompson, 2022). The central positioning of schools in community development is emphasised by the role of teaching learners' essential ICT skills needed in the digital age, as well as guiding parents regarding learners' internet use at home (Delgado, Wardlow, Mcknight, & Malley, 2015; Rahman, Sairi, Zizi & Khalid, 2020). The integration of ICTs in the school system also implies that schools are custodians of huge amounts of data including personalinformation of learners, parents, educators, and administrative staff, highlighting the importance of cybersecurity in schools (Richardson, Lemoine, Stephens & Waller, 2020). Cyber-criminals continually target sensitive, private, and financial information of different stakeholders in the custody of schools. Thus, management buy-in is essential if a school is to prioritise cybersecurityin terms of both awareness and the development of cybersecurity educational programs (Tsado, 2019).

In the South African context, the management role of the principals is shared among school management teams (SMTs) which often include deputy principal(s) and head of sections within aschool system (Madimetsa & Saltiel, 2021). SMTs carry out multifaceted challenging anddemanding roles, with the digital age demanding more from them than what is normally expected (Mestry, 2017; Mahlangu, 2018). The increased use of computer connectivity within the school context meant a growth of digital information, which is much more difficult to protect than hard copy files (Aleroud & Zhou, 2017). The COVID-19 pandemic exacerbated the situation as SMTs, educators and learners from resource-constrained schools lacked the required digital literacy skills and ICTs needed to sustain teaching and learning during the imposed lock down periods (Dube, 2020). Yet, ICTs have since been proven to be an integral part of the school systems as their use in curriculum delivery and data management is inevitable. SMTs should, therefore, take on the responsibility of cybersecurity within the school. Rural and high-density schools, described as resource-constrained schools in this study, may be more uniquely disadvantaged in addressing cybersecurity issues since they have limited resources to invest in cybersecurity (Sheasley, 2020).

Cybersecurity entails the mechanisms of protecting individuals' and an institution’s assets from unauthorised access closely linked to protection and privacy and the confidentiality, integrity, and availability of digital information (Torres & Thompson, 2020). The high penetration of new technologies in Africa and the low priority on cybersecurity by most countries on the continent, increases the exposure to cyber-threats in educational institutions due to the complexities of diverse populations who misuse ICTs (Aliyu, Abdallah, Lasisi, Diyar & Zeki, 2010).

Schools have not focused on cybersecurity to the same extent as industries and businesses hence they find themselves ill-prepared for cyber-attacks (Goldsborough, 2016). Resource-constrained schools generally operate under limited resources hence they may face challenges in developing measures to counter cyber-threats. Therefore, such schools are more susceptible and vulnerable to cyber-attacks (Chigona, Mudavanhu, Siebritz & Amerika, 2016; Sheasley, 2020). Nonetheless,SMTs in marginalised schools should have the capabilities to assess the risks associated with theuse of ICTs. They can achieve this by being aware of their vulnerabilities, their weaknesses, and the potential repercussions of a successful attack on their goals and those of the various school stakeholders (Bureau of Cyber Statistics, 2023).

An understanding of SMTs cybersecurity perception within a school context can help highlight existing levels of cybersecurity knowledge and awareness among school leadership thereby providing a base for ICTs and education authorities to provide appropriate cybersecurity trainingand interventions for school management. Perception refers to an "individual’s construction of his or her reality, thus, there is potential for perceptions to be affected by an individual’s self-concept"(Crandall, Noteboom, El-gaya

& Crandall, 2019:75). Cybersecurity perceptions and personal experiences can vary depending on an individual's knowledge levels, and the dynamic nature of cyber threats within one's context (Maisikeli, 2020). This study, therefore, contributes to cybersecurity in education by answering the question:

What are the perceptions of cyber-threats among school management in resource- constrained schools?

The objective of the study is to examine the cybersecurity perceptions of school managers in resource-constrained schools in South Africa. The findings of the study would pave way for initiatives that would capacitate cybersecurity knowledge and skills among school managers in resource-constrained schools and, in turn, cultivate a culture of cyber safety in these schools. Thestudy explores how societal structures, location factors, and personal characteristics affect schoolmanagement self-efficacy as they deal with cybersecurity related matters in the leadership role. The South African context offers an ideal context for the study because of its distinct economic disparity which is a legacy of the country's apartheid history. Further, the country has one of thehighest ICT penetration and deliberate government policies to provide ICTs in schools (Dlamini & Coleman, 2017). The sample for the study is drawn from the Western Cape and Limpopo provinces. The former is regarded as an affluent province; while the latter is economically challenged (Turok, 2018). Schools are governed by their respective provincial departments of education.

2 Literature Review

The social, economic, and political integration of all South Africans, particularly those excluded under apartheid, was the top priority on the national agenda in the years following the country's political transition (Spaull, 2013). Education was prioritised as an area of reform and growth (Harber, 2001; Chisholm, 2005). Nonetheless, due to the legacy of apartheid many former "non-white" schools in rural areas, former townships and informal settlements face numerous resources- constraints. Within the political arena there were also concerns after attaining democracy that SouthAfrica's rural areas and former townships were marginalised and under-resourced (Gunzo & Dalvit,2012).

Townships have historically been linked to an institutionalised, racially discriminatory system of migrant labour, while the informal settlements that have sprung up in metropolitan areasover the past 25 years have been seen as another legacy of the apartheid era (Burger, Van der Berg,Van Der Walt & Yu, 2017). These urban settlements are generally associated with high unemployment rate, inadequate infrastructure, poor administration, high uncontrolled population densities with increased cases of substance abuse and crime (Chikoto, 2010). Similarly, rural areas are generally remote and relatively underdeveloped, as a result, many schools lack the necessary physical resources and basic infrastructure for sanitation, water, roads, transport, electricity, and ICTs (du Plessis & Mestry, 2019). Despite these challenges, the use of ICTs in schools is on the increase with a growing number of learners using ICT devices at school, including cell phones, tablets, and computer labs (Shambare, Simuja & Olayinka, 2022). The Department of Basic Education's Quintile System determines the state of a school being regarded as resource-constrained (White & Van Dyk, 2019). The quintile system classifies schoolsinto five categories, ranging from the poorest (Quintile 1) to the least poor (Quintile 5). Government financial support is allocated based on the quintiles. Quintile 1 schools receive the highest allocation per learner and Quintile 5 receive the lowest (CAPS 123, 2023). Schools in rural and low-income high-density suburbs usually fall between Quintile 1 and Quintile 3. Learners inschools in Quintiles 1 to 3, often are not required to pay tuition fees.

According to the South African law, the well-being and safety of learners on the school grounds is the responsibility of the school. This responsibility includes cyber-safety awareness especially when schools provide access to ICT devices (De Lange & von Solms, 2012). Schools are

custodians of invaluable large data sets that are highly regarded in the cyber marketplace (Richardsonet al, 2020). SMTs have the responsibilities that include ensuring the best possible resourceachievement, allocation and evaluation, and the security of the site whilst the management of teaching and learning remains one of the fundamental activities for the school leadership (Bush, Kiggundu & Moorosi, 2011). However, as custodians of a school, SMTs have the responsibility of ensuring the cybersecurity of the school assets and various stakeholders within the school system. Such stakeholders include learners, educators, parents, and their personal information. Cyber risks can have social implications on the stakeholders in the school context as they include crimes such asfraud, identity theft, cyber-bullying, sextotion, and grooming (Kritzinger, 2017). Thus, in addition totheir daily management duties, the digital age demands that SMTs have knowledge on cybersecurityrisk management which involves being able to identify, protect against potential cybersecurity incidents, detect, respond to recover from actual cybersecurity incidents (Bureau of Cyber Statistics,2023).

Schools do not typically invest resources to handle cybersecurity at the same level as government and big business (Goldsborough, 2016). As a result, South African schools have had little exposure to cybersecurity initiatives to improve cyber-safety within schools (Kortjan & von Solms, 2014). Rural and low-income urban schools are more vulnerable to cyber-attacks since they operate with limited resources (Kritzinger, 2020). Limited cybersecurity knowledge within a schoolmeans the various stakeholders can easily succumb to various cybersecurity threats and risks as theybecome easy targets for hackers (Sawyer & Hancock, 2018). School leadership should be knowledgeable about cybersecurity to provide the required protection, support, and management of cybersecurity within schools. SMTs, therefore, need to have a high self-efficacy as they deal with cybersecurity related matters within a school context.

Cybersecurity attitudes, values, and practices of internet users are influenced by socio- cultural factors (Creese, Dutton & Esteve-Gonzalez, 2021). The skills and understanding of cybersecurity as well as the experiences, perceptions, attitudes, and beliefs of school managers influence their behaviour and, therefore, their response to a cybersecurity related matters within a school set-up. In this study we regard perceived self-efficacy for a member of a school managementteam to be the assurance and capacity that one possesses to sustain challenges and mobilise requiredresources to meet the demands of a cybersecurity situation. Self-efficacy is, therefore, understood inthis study as an individual's confidence in their ability to perform a task (Graham, 2022).

3 Theoretical Framework

The study employed the Capability Approach theory. The key characteristic of the theory is its emphasis on people's ability to attain the goals they value (Frediani, 2010). The Capability Approach recognises that societal structures, location factors, and personal characteristics affect an individual's ability to convert goods into worthwhile accomplishments (Sen, 1985). Thus, the approach focuses on people's capability of doing and being, considering the resources they have access to. In terms of cybersecurity in schools, this entails the capability of stakeholders in schools to use the resources and knowledge available to them to be safe and secure as they use the internet.

The Capability Approach is based on two basic concepts of functionings and capabilities. Functioning is an umbrella term for the resources, activities, and attitudes that individuals instinctively value such as gracefulness, knowledge, close relationships, education, and a fulfillingcareer (Alkire, 2003). These actions and states of being and doing are, therefore, referred to as"achieved functionings," and they are what give an individual's life meaning and sense offulfilment (Kuhumba, 2018). In a school setting the instinctive need to ensure the cybersafety ofthe stakeholders under the custodianship of a school manager can be considered as a functioning.

Capabilities are the doings and beings that individuals can attain if they so desire, such as being well-nourished, getting married, and travelling (Sen, 1985). Thus, functioning is actual

achievements, and capabilities are effective freedom (Gasper, 2002). A person's capability denotestheir effective freedom to select between various functional combinations and between various lifestyles that one values. Therefore, a person's attained functioning is those they consciously choose, and their capability set is the collection of valuable functionings to which they have actualaccess (Robeyns, 2005). Thus, stakeholders within a school context with the required cybersecurity resources, knowledge and skills can have cybersecurity capabilities to ensure effective cyber hygiene practices.

````Since capabilities represent freedoms in the sense that they are corrected for any potential impediments, functionings simply denotes those capabilities that have been achieved whether voluntarily or by chance (Robeyns, 2005). Sen uses “capability” not to refer exclusively to a person’s abilities or other internal powers. Rather, the term isused to refer to an opportunity madefeasible, and constrained by, both internal (personal) and external (social and environmental) conversion factors. Social conversion factors are elements from the society in which one lives, such as public policies, social norms, or power relations, environmental conversion factors emerge from constructed surroundings in which an individual resides and personal conversion factors are internal to the person, such as metabolism, physical condition, reading skills, or intelligence (Kuhumba, 2018).

Agency and well-being are important concepts within the capability approach. Agency entails the freedom of the individual to select and bring about the things that they value (Mahlo & Waghid, 2022). It also includes states of affairs that do not always promote one’s well-being (Sen, 1995). In the digital age, therefore, limited cybersecurity knowledge can lead to exposure tocyber-attacks which is detrimental to one’s well-being. Well-being involves an evaluation of everything related to a person's circumstances, or an evaluation that is centred on the person's existence (Gasper, 2002). It is expressed though freedom and a happy life (Sen, 1995). Sen, however, distinguishes "well-being” from the pursuit and fulfilment of one's goals and obligations, and instead limits it to one's personal gratification. Conversely, he defines agency as the ability ofan individual to pursue and realise one’s values and has reason to value, or, in other words the freedom to establish and follow one's own goals and interests (Sen, 1985). Thus, the ability of school managers to ensure the well-being of those under their guardianship through cyber safety is of importance in schools.

In Sen’s viewpoint, it is important to view human growth as a process of increasing people's capabilities. We employed the capability approach in this study because it deliberately considers personal factors, environmental conditions, social pressures as factors affecting how the use of resources gets converted into desired capabilities. These factors allow us to explore the roleof school management in resource-constrained environments as they respond to the demands of the digital age and their role as school custodians as far as cybersecurity is concerned. Table 1 shows the capability approach concepts used in this study.
````

Construct	Explanation
Commodity/resource	The characteristics and availability of technology and relevant cybersecurity knowledge
Conversion factors	Personal factors e.g. training Social factors e.g. social institutions, social norms, politics, environmental factors e.g. infrastructure, resources
Agents	Whose capabilities are deprived? e.g. educators, learners, parents, vendors, other stakeholders
Capabilities	The capabilities the learners and educators are deprived of well-being, freedom: e.g. education, utilisation of technology etc. Agency freedom e.g. taking advantage of available resources, policy making

Table 1: Concepts for unpacking ICT and its limited use (Zheng &Walsham, 2008)

4 Methodology

Using purposive sampling, we chose four schools evenly from rural and urban resource-constrained schools from Limpopo and Western Cape provinces. The sample for the study consistsof eight members of the SMT that include principals, deputy principals, and heads of departmentsof the selected schools. We collected the data through semi-structured in-depth interviews from consenting participants. We collected the data between April and September 2023. The data wasanalysed through qualitative thematic analysis. We followed a deductive approach by applying themes from the Capability Approach and literature on the data to identify instances that match the predefined themes (Fereday & Muir-Cochrane, 2006).

Ethical clearance for the study was obtained from the researchers' institution. To maintain confidentiality and anonymity, pseudonyms were employed for the four schools in the study. Theschools from the Western Cape are identified as WC-A and WC-B; the schools from Limpopo are identified as LMP-A and LMP-B. The respondents are identified by a code which represents theirschool and their respective serial numbers.

4.1 Case Description

Table 2 summarises the statistics of the sampled schools. All the schools in the sample are non-fee paying which depend on government for support

Province	School	Location	Learners	Educators	SMT
Western Cape	WC-A	Urban	1600	48	8
	WC-B	Rural	620	24	5
Limpopo	LMP-A	Urban	1188	34	8
	LMP-B	Rural	1100	29	6

Table 2: Summary of the statistics of the sampled schools

WC-A school is located 17km from Cape Town (provincial capital of Western Cape). The school is a high- density suburb that has since been overwhelmed by a sprawling informal settlement. The settlement is characterised by poverty, high crime and unemployment rates, and substance abuse. WC-B is located in a small farming town 187km from Cape Town. The challenges in the small town include high illiteracy rates, poverty, and substance abuse.

LMP-A is an urban school located 15km from the city of Polokwane (the provincial capital of Limpopo). The school is in a low-income high-density suburb characterised by high crime and unemployment rates, substance abuse and poverty. LMP-B is located 290km from Polokwane. The school is in a subsistence farming rural setting. The community has high unemployment, illiteracy rates and poverty.

5 Empirical analysis and Discussion.

This segment is presented in three sections: environmental factors, social condition, and capabilitiesin the face of cyber threats within the school setting. Environmental factors include the infrastructure and resources within the school contexts that affect school managers' cybersecurity self-efficacy and capabilities. Social conditions are the instruments available to school managers that enable their cybersecurity functioning and capabilities such as cybersecurity policies, practices,and data management systems.

5.1 Environment Factors affecting school managers cybersecurity self-efficacy and capabilities

The respondents emphasised the importance of having adequate financial resources to provide adequate technological devices that would improve their cybersecurity functionings. They regardedthe shortage of financial resources in their environments as hindering their capability to ensure cybersecurity in schools. *"It's difficult to be safe on the internet. It requires great sums of money"* (WC-B1). "*We have 34 educators, if we had the money, we would adopt 'one teacher-one laptop' approach* (LMP-A1). The respondents demonstrated a narrow understanding of cyber risks; they perceived that cyber risks would arise primarily from sharing technological resources and that the way to mitigate this would be to have enough hardware resources so that the educator do not share laptops. The techno-deterministic view on cybersecurity failed to look at the broader cybersecurity measures that can be achieved where technological devices must be shared due to resource-constraints.

The respondents perceived that their environment limited their cybersecurity capabilities:

"We *have nothing. We are far behind. I am scared because we know nothing"* WC-A2.

"*… because the environment that we are in is not conducive…. Isn't it that we areregarded the poorest of the poor"* (LMP-B2).

The school managers cybersecurity self-efficacy is affected by the political and economic narrative in the South African context that regard rural and urban low-income suburbs as poor and marginalised and, therefore, in need of government and well-wishers' support. Since the school managers perceived themselves to be poor, their negative self-perception led to low cybersecurity self-efficacy. They believed their environmental conditions were responsible for their lack of cybersecurity resources and knowledge which exposes their schools to cyber-attacks. In addition, they believed that the social ills of their communities affected their cybersecurity capability and self-efficacy; they mirrored their fear of crime in the high crime zones the schools are located to the cyberspace. *"We are not safe physically and online"* (WC-A1).

5.2 Social Conditions affecting school managers cybersecurity self-efficacy and capabilities.

The capability approach emphasises policies as they provide an enabling environment that give individuals agency and the freedom to choose for their well-being (Mahlo & Waghid, 2022). In thiscase, cybersecurity policies in schools would ensure cyber safety and cyber hygiene for the various stakeholders in the school context. However, the capability of stakeholders in rural and resource-constrained schools was compromised by the absence of policies *"The school does not have any policies"* (LMP-A2); *"we do not have one (policy)"* (LMP-B1). The respondents were aware thatthe absence of cybersecurity policies affect their capability to be safe in the cyberspace, However,they felt helpless since "*... we have got nothing in place to protect us"* (WC-A2).

Of note is how respondents mixed up the "an ICT policy" and "cybersecurity policy" for a school.

"We've organised a team to develop the policy on how we're going to implement cybersecurity, where there are devices that we don't allow our learners to come to school with because they disrupt lesson. We need to guard against being behind with the syllabusand not being disturbed by other activities" (WC-A1).

Such respondent's statements demonstrated limited understanding and knowledge of cybersecurity;they believed controlling the use of technological devices in the classroom is cybersecurity. Despite the blatant misunderstanding, the statement highlights the perception of the school manager that cybersecurity is not a priority in the school. Rather the focus of the school is completing the syllabus on time, which is a measurable key performance area. However, the school managers failed to appreciate that cybersecurity has a positive well-being, more so for learners, who are the most vulnerable in the school's context.

In some cases, school managers responses to cybersecurity issues in schools was obligatoryas a reaction to their superiors' directives and not a functioning of their sense of responsibilities towards data management. *"Yes, we have that policy, but we have not done the implementation, it requires all the information about the school to be kept in one backup system for the department* (WC-B2). The school managers regarded the directive to digitise information by their respective provincial Department of Education within schools as policy. *"Last year the government rolled outthe POPI [Protection of Personal Information] Act and all the learners were in the hall and were informed"* (LMP-B1). Thus, the school managers lacked personal agency and capability to ensure cybersecurity within the schools *"we are not confident because we haven't gotten the proper training on the steps needed and the rules that govern information management*" (WC-A1).

SMTs efficacy is affected by the way the educational authorities failed to emphasise the need to equip them with cybersecurity capabilities through knowledge and skills. The South African education authorities have introduced management information systems for schools; Central Education Management Information System (CEMIS) in the Western Cape and South African School

Administration Management System (SA-SAMS) in Limpopo province (Maremi,Herselman, & Botha, 2020). However, school managers felt they were not prioritised on data management training:
"*It's the administration staff that goes for training on how to do data handling training on CEMIS" (*WC-B2).
"There are only three people who have access to SA-SAMS; we have a clerk and two educators in case the clerk is not available" (LMP-A1).
In cases of suspected data breach on the management information systems, school management "report to district office for support" (LMP-B2). However, instead of training them *"they come and fish for us and then we will be left not knowing what's happening and how to do it."* (WC-A2). The resource-constrained environment restricted school managers capabilities to ensure confidentiality, availability, and integrity of data "*because we do not have enough technicians, sometimes he is at another school in the district and say I will come when it is your turn*." (LMP- A1).

5.3 Capabilities in the face of cyber threats within the school

The cybersecurity capabilities of various stakeholders, most importantly the learners, were compromised by the limited cybersecurity knowledge of school management. Rural and resource-constrained schools faced cyberspace related challenges "some of our learners are bullied on Facebook but there's little we can do about it" (WC-B2). School managers' instinctive functioning to protect learners was restricted because they "*don't have information to tell learners how to behave on social media*" (LMP-B2). They felt helpless in the face of cyber threats and risks targeting learners *"they have phones and internet, when they are in trouble, I don't know what to do*" (WC-B1). Respondents recognised that their limited cybersecurity knowledge deprived learners of the capability to be safe in cyberspace "how can we teach somebody something that we don't know ourselves" (WC- A2).

Cyber threats within rural and resource-constrained schools did not only affect the well- being of learners but educators as well. Some educators were "*scammed of their salaries*" (WC-B1) or "lost their money though fraud" (LMP-A1). School managers, therefore, felt helpless when stakeholders within the school context were targeted by cyber-criminals. They realised their limitations as they lacked the knowledge and skills to impart to educators *"I don't know what I must tell them, apart from the fact that we are working in an ever-changing environment, and we must teach ourselves on how to move forward"* (WC-A1). The negative cybersecurity experience, highlighted to school managers the importance of cybersecurity training *"the rest of us must hit the ground running because we also need the workshops. If we had workshops, there will be in no way we can have fallen into the (online fraud) trap"* (LMP-B2).

6 Conclusion

The security and safety of learners, educators, parents, and administrative staff in the digital age are of utmost importance to school managers. Increasingly, school management is expected to take a lead in addressing cybersecurity related matters in a school context. Compromise on the cyber well-being of those under their guardianship has an impact on the school's mandate of delivering teaching and learning. Given their strategic positioning within the school system to oversee, support, and direct matters related to cybersecurity, school managers should have a comprehensive understanding of cybersecurity.

School managers, however, are aware of the cybersecurity vulnerabilities within their context and acknowledge their lack of cybersecurity capabilities and knowledge. At the same time, education and ICT authorities have not prioritised cybersecurity capacity building for school managers. This has exposed rural and resource-constrained schools and communities to cyber-attacks. We recommend that cybersecurity should be part of school managers continuous professional development. Provincial education department should not only prioritise school administrative staff on the use of School Management Systems, but rather school managers should also be equipped with knowledge and skills

on the management of data within their schools. The cybersecurity perceptions of resource-constrained school managers are, to an extent, informed by the political and economic narrative in the South African context that regard rural and low-income urban areas as poor and marginalised. Consequently, school managers perceive that their incapacities and limited capabilities in cybersecurity is caused by their limited financial resources to acquire the required ICTs and not due to the lack of capacity building for various stakeholders in the school system to ensure cyber safety and cyber hygiene practices. It is therefore imperative that rigorous cybersecurity awareness initiatives are provided in resource constrained schools to highlight the various ways internet users can be safe online even in cases where they must share digital resources.

The primary responsibility of school managers is ensuring teaching and learning. Ensuring cybersecurity within the school environment is not yet an explicit measurable key performance area for schools in South Africa. Consequently, cybersecurity is typically not given priority. This challenge could be addressed by education authorities making management of cybersecurity in a school a key performance area for school managers. Further, school managers could be made to appreciate the importance of cybersecurity on the primary goal of completing the curriculum. A cyber-threat could jeopardise effective completion of the curriculum.

One of the main roles of school managers is to ensure compliance of policies that provide standards, protocols, and guidelines of various aspects within the school system. However, because resource-constrained schools have limited cybersecurity expertise and knowledge, the schools do not have cybersecurity policies that would guarantee cybersecurity if adhered to in the school context. Whilst the DBE has a cybersecurity policy for schools. Education authorities should ensure that school managers are not only aware of the policy but are equipped to implement the policy in schools and if possible, to adapt the police and develop contextualised cybersecurity policies that address the needs of a particular school.

This study used a small sample size of four case studies from two provinces. We recommend that future studies use more case studies and a larger sample size of resource- constrained schools. We have noted that one of the main challenges facing school management in resource constrained schools is lack of knowledge. We recommend a design science study which would come up with the curriculum which would be bespoken for resource- constrained schools.

7 Acknowledgements

The authors would like to acknowledge the financial contribution of the National Research Foundation (NRF) in conducting this study as part of the research project entitled Cybersecurity framework for rural and disadvantage schools in South Africa.

References

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. In Computers and Security (Vol. 68, pp. 160–196). Elsevier Ltd. https://doi.org/10.1016/j.cose.2017.04.006

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010, December). Computer security and ethics awareness among IIUM students: An empirical study. In Proceeding ofthe 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010 (pp. A52-A56).

Alkire, S. (2003). The Capability Approach as a Development Paradigm? Development, 7(September), 1–18 http://www.capabilityapproach.com/pubs/461CAtraining_Alkire.pdf

Bureau of Cyber Statistics (2023) Congressional research Services https://sgp.fas.org/crs/misc/R47389.pdf

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.

Bush, T., Kiggundu, E., & Moorosi, P. (2011). Preparing new principals in South Africa: The ACE: School leadership programme. South African Journal of Education, 31(1), 31–43. https://doi.org/10.15700/saje.v31n1a356

CAPS 123 (2023). Understanding School Fees and Quintiles in South African Public School.https://caps123.co.za/understanding-school-fees-and-quintiles-in-south-african-publicschools/#:~:text=The%20quintile%20system%20in%20South,that%20may%20not%20charge%20 fees

Chigona, W., Mudavanhu, S. L., Siebritz, A., & Amerika, Z. (2016). Domestication of free Wi-Fi amongst people living in disadvantaged communities in the Western Cape province of South Africa. Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists, 1–9.

Chikoto, T. (2010). Informal Settlements in South Africa https://repository.up.ac.za/bitstream/handle/2263/14436/Chikoto_Informal(2009).pdf?sequence=1

Chisholm, L. (2005). The politics of curriculum review and revision in South Africa in regional context.

Compare, 35(1), 79–100. https://doi.org/10.1080/03057920500033563

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

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. https://doi.org/10.1007/s00779- 021-01569-6/Published.

De Lange, M., & Von Solms, R. (2012). An e-Safety educational framework in South Africa. In Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC).

Delgado, A. J., Wardlow, L., Mcknight, K., & Malley, K. (2015). Educational technology: A review of the integration, resources, and effectiveness of technology in K-12 classrooms. In Journal of Information Technology Education: Research (Vol.14). http://www.jite.org/documents/Vol14/JITEv14ResearchP397-416Delgado1829.pdf

Dlamini, R., & Coleman, E. (2017). ICT in Education. South African Computer Journal, 29(2), vii-x.du Plessis, P., & Mestry, R. (2019). Teachers for rural schools – A challenge for South Africa. South African Journal of Education, 39. https://doi.org/10.15700/saje.v39ns1a1774

Dube, B. (2020). Rural Online Learning in the Context of COVID-19 in South Africa: Evoking an Inclusive Education Approach. 10(2), 135–157. https://doi.org/10.4471/remie.2020.5607

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

Frediani, A. A. (2010). Sen's capability approach as a framework to the practice of development. Development in Practice, 20(2), 173–187. https://doi.org/10.1080/09614520903564181

Gasper, D. (2002). Is Sen's capability approach an adequate basis for considering human development? Review of political economy, 14(4), 435-461.

Goldsborough, R. (2016) Protecting yourself from ransomware. Teacher Librarian, 43(4), 70.

https://doi.org/10.1080/0953825022000009898.
Graham, S. (2022). Self-efficacy and language learning–what it is and what it isn't. Language Learning Journal, 50(2), 186–207. https://doi.org/10.1080/09571736.2022.2045679
Gunzo, F. & Dalvit, L. (2012). A survey of cell phone and computer access and use in marginalised schools in South Africa. Proceedings of M4D 2012 28-29 February 2012 New Delhi, India 28
Harber, C. (2001). Schooling and violence in South Africa: creating a safer school. Intercultural education, 12(3), 261-271.
Kortjan, N., Von Solms, R., & Box, P. O. (2013). Cyber Security Education in Developing Countries:A South African Perspective. In LNICST (Vol. 119).
Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. South African Computer Journal, 29(2), 16–35. https://doi.org/10.18489/sacj.v29i2.471
Kritzinger, E. (2020). Improving cybersafety maturity of South African schools. Information (Switzerland), 11(10), 1–17. https://doi.org/10.3390/info11100471
Kuhumba, K. S. (2018). A Review of Amartya Sen's Re-examination of Inequality. Sustainable Development, 9(1).
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
Mahlangu, V. P. (2018). Pertinent leadership and governance challenges facing schools in South Africa. Education in Modern Society, 16, 136–142.
Mahlo, L., & Waghid, Z. (2022). Examining information and communication technology use in public primary schools in South Africa from the capability approach. The Journal for Transdisciplinary Research in Southern Africa, 18(1). https://doi.org/10.4102/td.v18i1.1201
Maisikeli, S. (2020). UAE cybersecurity perception and risk assessments compared to other developed nations. Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020, 432–439. https://doi.org/10.1109/ICICT50521.2020.00075
Maremi, K., Herselman, M., & Botha, A. (2020). Scoping the aspects and capabilities of South African School Administration and Management Systems (SA-SAMS). In 2020 Conference on Information Communications Technology and Society (ICTAS) (pp. 1-6). IEEE.
Mestry, R. (2017). Empowering principals to lead and manage public schools effectively in the 21st century. South African Journal of Education, 37(1), 1–11. https://doi.org/10.15700/saje.v37n1a1334
Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393
Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Educational Planning (Vol. 27, Issue 2).
Robeyns, I. (2005). The Capability Approach: a theoretical survey. Journal of Human Development, 6(1), 93–117. https://doi.org/10.1080/146498805200034266
Sawyer, B. D., & Hancock, P. A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. Human Factors, 60(5), 597–609. https://doi.org/10.1177/0018720818780472
Sen A. (1995) Inequality re-examined. Cambridge, MA: Harvard University Press
Sen, A.K. (1985). Commodities and Capabilities, Oxford: Elsevier Science Publishers.
Shambare, B., Simuja, C., & Olayinka, T. A. (2022). Educational technologies as pedagogical tools: Perspectives from teachers in rural marginalised secondary schools in South Africa. International Journal of Information and Communication Technology Education (IJICTE), 18(1), 1-15.
Sheasley, C. (2020). As remote learning spreads, so have cyberattacks. Are schools ready? The

Christian Science Monitor. https://www.csmonitor.com/USA/Education/2020/1103/As-remote-learning- spreads-so-have-cyberattacks. -Are-schools-ready

Spaull, N. (2013). Poverty & privilege: Primary school inequality in South Africa. International journal of educational development, 33(5), 436-447.

Taylor, S. (2011). Uncovering indicators of effective school management in South Africa using the National School Effectiveness Study. Stellenbosch Economic Working Papers, 1–51.

Torres, M., & Thompson, N. (2020). Toward a Cyber Security Adoption Framework for Primary and Secondary Education Providers.

Tsado, L. (2019). Cybersecurity Education: The need for a top-driven, multidisciplinary, school-wide approach. Journal of Cybersecurity Education, Research and Practice, 2019(1), 4.

Turok, I. (2018). Worlds apart: spatial inequalities in South Africa. Confronting inequalities in South Africa, 159-182.

White, C. J., & Van Dyk, H. (2019). Theory and practice of the quintile ranking of schools in South Africa: A financial management perspective. South African Journal of Education, 39(Supplement 1), 1-19.

Zheng, Y., & Walsham, G. (2008). Inequality of what? Social exclusion in the e-society as capability deprivation. Information Technology and People, 21(3), 222–243. https://doi.org/10.1108/09593840810896000