Cybersecurity for Marginalised Schools in South Africa – Cy4MaS

Executive Summary

As schools increasingly embrace digital platforms for learning, administration, and communication, in the 21st century, there is greater need for a robust cybersecurity framework. The cyberspace presents countless opportunities for schools; however, they are also prone to a growing number of cyber threats, including ransomware, data breaches, and unauthorized access to sensitive information to school stakeholders that include learners, parents and staff. The cyberspace exposes school stakeholders to cyber threats such as cyber bullying, sextortion and phishing attacks. The proposed Cybersecurity for Marginalised Schools Model (Cy4MaS) offers a comprehensive and adaptive solution to safeguard the digital ecosystem of educational institutions.

CY4MAS constitutes the standards, guidelines, and best practices for a school to better manage and reduce cybersecurity risk. The model outlines the security requirements that should be in place if a school is to be safe from cyber-attacks. The model outlines five dimensions:

School Cybersecurity Policy and Strategy

School Cybersecurity Culture

School Cybersecurity Training and Skills

School Cybersecurity Legal and Regulatory Compliance

School Cybersecurity and Standards and Technologies

The South Africa cybersecurity policy aims to create a secure cyberspace and a knowledgeable society that understands and that can protect itself from cyber-related threats (Government of South Africa, 2015). Loosely based on the Cybersecurity Maturity Model for Nations – CMM (GCSCC, 2021), Cy4MaS is scalable and can be customised by schools to fit their unique technological landscapes and resource constraints. Its implementation does not only emphasis investment in information technologies but is a critical step towards maintaining the trust of the school's stakeholders while safeguarding the institution's mandate of teaching and learning.

Using the Cy4MaS Model, schools can create a secure digital environment that enables innovation and learning without compromising data privacy or operational continuity. The dynamic nature of the cyberspace requires continuous monitoring to address emerging threats, technology changes, and evolving educational needs through the involvement of the school community through a bottom-up Community of Purpose Cybersafety for Marginalised Schools Model.

Table of Contents

Glossary of Acronyms

C3SA	Cybersecurity Capacity Centre for Southern Africa
CEMIS	Centralised Educational Management Information System
CMM	Cybersecurity Capacity Maturity Model for Nations
Cy4MaS	Cybersecurity for Marginalised Schools in South Africa
DBE	Department of Basic Education
ECTA	Electronic Communication and Transaction Act
GCSCC	Global Cyber Security Capacity Centre
ICTs	Information and Communication Technologies
LURITS	Learner Unit Record Information and Tracking System
PAIA	Promotion of Access to Information Act SAPS South Africa Police Service
PDE	Provincial Department of Education
POPI	Protection of Personal Information Act
RCL	Representative Council of Learners
SASAMS	South African School Administration and Management System
SGB	School Governing Body
SMT	School Management Team
UCT	University of Cape Town
UL	University of Limpopo
VPN	Virtual Private Network

Terms and Definitions

Cyber Crime - an offence that can only be committed using a computer, computer networks or other forms of ICTs

Cyber Risk - the potential of exposing an ICT system to actors, elements and circumstances able to cause loss and damages

Cybersecurity - a field of study and practice focusing on protecting people and organised entities, critical computer systems, and sensitive information from digital attacks, threats and risks

Cyber threat - any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, or other entities through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service

Crisis management - plan and a practice for an organisation to respond to and recover from disturbing, damaging, and destructive events

Cryptographic controls - security measures aiming at protecting data using encryption and decryption techniques and technologies

Incident response - a strategic plan and practice of identifying and mitigating the effects of a cyber-attack on an organisation's ICT assets

School ICT/Internet Infrastructure - the collection of hardware, software, networks, and other systems that enable the communication of data and information

Security controls - security controls are the safeguards and countermeasures that organizations put in place to protect digital assets and information from cyber threats. These controls are designed to mitigate risks, prevent attacks, detect intrusions, and ensure the confidentiality, integrity, and availability of data

Introduction

e-Learning has provided unrivalled opportunities for learners and educators to access and deliver learning material/content. However, this development has not been without a dark side. Learners and schools are exposed to a plethora of cyber threats. Threats like cyber-bullying and cyber-harassment have become topical issues in South Africa (SA) and have notably been increasing at an alarming rate. Schools are generally custodians of large data sets. They hold personal data about the school's stakeholders such as learners and their guardians (e.g. identification numbers, e-mail addresses, credit card details, financial data, and other personally identifiable information). They are a target of malicious attacks.

School stakeholders should have the requisite knowledge of the threats, vulnerabilities, and possible mitigation strategies. However, marginalised schools and their stakeholders struggle to achieve cyber resilience against such threats and risks. Most stakeholders from marginalised schools tend to have limited awareness of cyber threats and risks which their online activities expose them to. Therefore, they would benefit from a guiding model that would help them to achieve cyber resilience.

The Cybersecurity for Marginalised Schools (Cy4MaS) aims to guide marginalised school towards cyber resilience. The model can also be used as a self-assessment tool for cybersecurity posture for schools.

Cy4MaS describes the evolution of a school's cybersecurity posture from a startup

stage to an established stage. Cy4MaS conceptualises a school as an ecosystem inter alia learners, educators, the administrative staff, community stakeholders, the premises, administrative and governance structures, the cyberspace, ICT infrastructure and related equipment.

When using the model schools can collect data through document review, interviews, focus groups and surveys for the various stakeholders. The data would be analysed using qualitative data analysis and descriptive statistics methods.

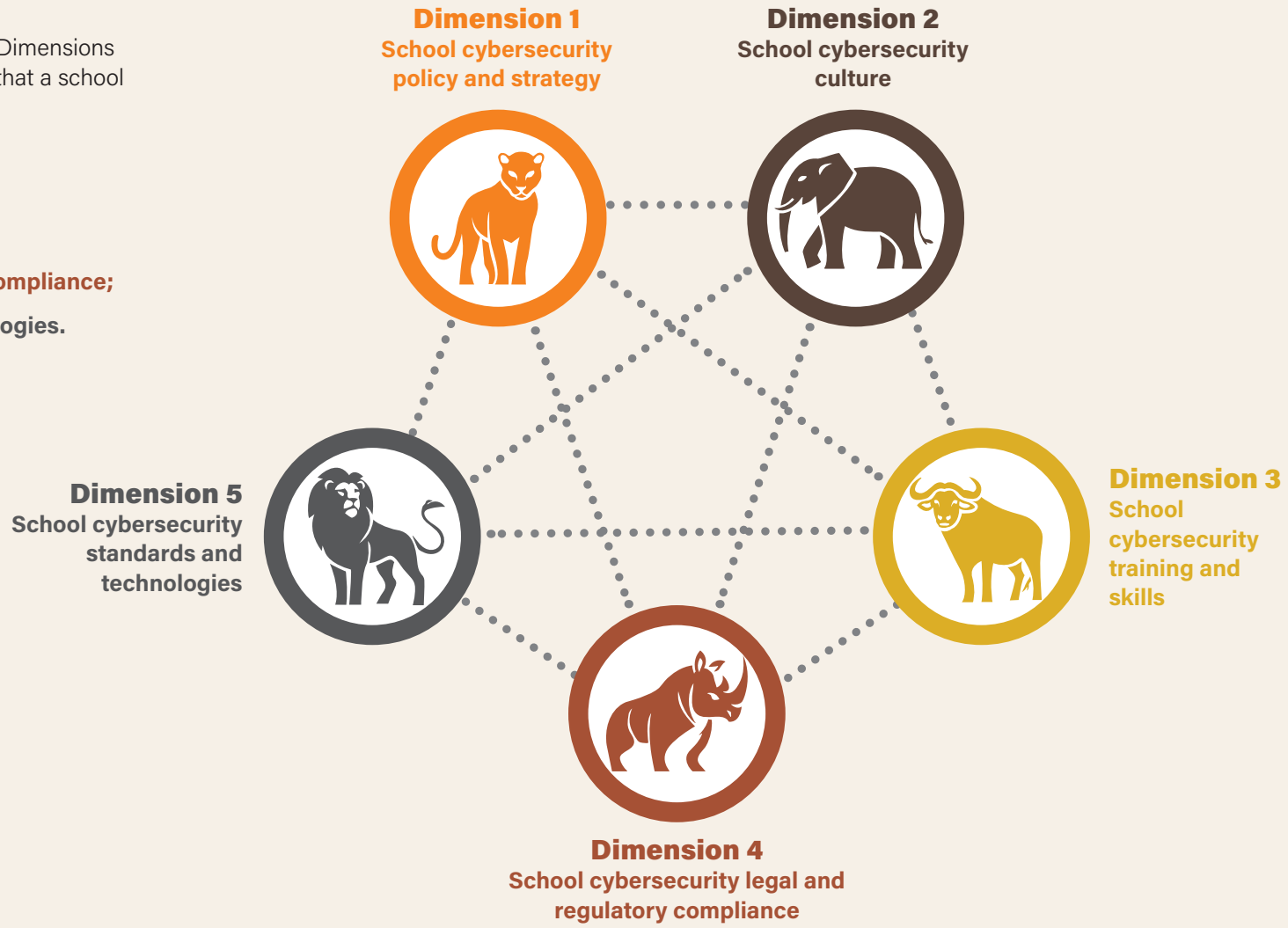
The outcome of analysis can be collated to determine the cybersecurity posture of the school and recommend remedial action.

This document presents the structure of the Cy4MaS model, and a description of the stage of cybersecurity development, before presenting the model in its dimensions, factors and aspects.

The Dimensions of Cybersecurity for Marginalised Schools (Cy4MaS)

Cy4MaS considers cybersecurity to comprise five Dimensions which together constitute the breadth of capacity that a school requires to be effective in delivering cybersecurity:

1. School cybersecurity policy and strategy;
2. School cybersecurity culture;
3. School cybersecurity training and skills;
4. School cybersecurity legal and regulatory compliance;
5. School cybersecurity standards and technologies.



Cybersecurity for Marginalised Schools in South Africa – Cy4MaS

The Cy4MaS considers cybersecurity to comprise five Dimensions, which constitute the breadth of capacity that a school requires to be effective in delivering cybersecurity:

Dimension 1: School Cybersecurity Policy and Strategy

Dimension 1 explores the school's capacity to access and deliver cybersecurity policy and strategy, and to enhance its cybersecurity resilience by improving its incident response, ICT infrastructure protection capacities. This Dimension considers effective strategy and policy in delivering School cybersecurity capability, while maintaining the benefits of a cyberspace vital for the community and society in general.

Factor 1.1: School Cybersecurity Policy

Factor 1.2: School Incidence Response and Crisis management

Factor 1.3: School ICT infrastructure protection

Factor 1.4: Cybersecurity in School security

Dimension 2: School Cybersecurity Culture

Dimension 2 reviews important elements of a responsible cybersecurity culture such as understanding of cyber threats and risks, the level of trust in Internet services, School online platforms, and users' understanding of personal information protection online. Moreover, it explores the existence of reporting mechanisms to report cybercrime as well as the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

Factor 2.1: Cybersecurity mindset

Factor 2.2: Trust and Confidence in Online Services and School Online Platforms

Factor 2.3: School stakeholders' understanding of personal information protection Online

Factor 2.4: Reporting Mechanism (Whistle Blowing)

Factor 2.5: Social Media and School Online Platforms

Cybersecurity for Marginalised Schools in South Africa – Cy4MaS

Dimension 3: School Cybersecurity Training and Skills

Dimension 3 reviews the availability, quality and uptake of programmes for various groups of school stakeholders, and relate to cybersecurity awareness-raising programmes, formal and informal training programmes for school.

Factor 3.1: Cybersecurity training

Factor 3.2: Digital literacy and cybersecurity skills

Dimension 4: School Cybersecurity Legal and Regulatory Compliance

Dimension 4 examines the school's capacity to comply with national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime legislation and other related legislation. Moreover, this Dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.

Factor 4.1: Policy and regulatory requirements

Factor 4.2: Related policy frameworks

Factor 4.3: Co-operation Frameworks to Combat Cybercrime at Schools

Dimension 5: School Cybersecurity Standards and Technologies

Dimension 5 addresses effective and widespread use of cybersecurity technology to protect school cyber-users, structures and ICT infrastructure. This Dimension specifically examines the implementation of cybersecurity standards and good practices, and the deployment of processes and controls, in order to reduce cybersecurity risks.

Factor 5.1: Adherence to PED/NED cybersecurity standards for schools

Factor 5.2: Security Controls

Factor 5.3: Software Quality and Internet Infrastructure Resilience

The Structure of Cy4MaS

Dimension

The five Dimensions together cover the breadth of assessed School cybersecurity by Cy4MaS. Each Dimension is constituted by a range of Factors, which capture the core capacities required to deliver the Dimension. Together, they represent the different 'lenses' through which cybersecurity capacity can be evidenced and analysed.

Factor

Within the five Dimensions, Factors describe what it means to possess cybersecurity capacity. These are the essential elements of school capacity, which are then measured for the maturity Stage. The complete list of Factors seeks to holistically incorporate all of a school's cybersecurity capacity needs. Most Factors are composed of Aspects which structure the Factor's Indicators into more concise parts (which directly relate to evidence gathering and measurement). However, some Factors that are more limited in scope do not have specific Aspects.

Aspect

Where a Factor possesses multiple components, these are Aspects. Aspects are an organisational method to divide Indicators into smaller clusters that are easier to comprehend. The number of Aspects depends on the themes that emerge in the content of the Factor and the overall complexity of the Factor.

Stage

Stages define the degree to which a school has progressed in relation to a certain Factor or Aspect of cybersecurity capacity. Cy4MaS consists of three distinct Stages of maturity: start-up, formative and established (detailed on page 9). A Cy4MaS review will benchmark a school against these Stages, capturing existing cybersecurity capacity, from which a school can improve or decline depending on the actions taken (or inaction). Within each Stage there are a number of Indicators which a school has to fulfil to successfully have reached the Stage.

Indicator

Indicators represent the most basic part of Cy4MaS's structure. Each Indicator describes the steps, actions, or building blocks that are indicative of a specific Stage of maturity. To have successfully reached a Stage of maturity, a school will need to convince itself that it can evidence each of the Indicators. To elevate a school's cybersecurity capacity maturity, all the Indicators within a particular Stage will need to have been fulfilled.

Most of these Indicators are binary in nature, i.e., the school can either evidence it has fulfilled the Indicator criteria, or it cannot provide such evidence.

Stages define the degree to which a school has progressed in relation to a certain Factor or Aspect of cybersecurity capacity. A Cy4MaS review will benchmark a school against these Stages, capturing existing cybersecurity capacity.

The Stages of the Cybersecurity for Marginalised Schools Model

Start-up

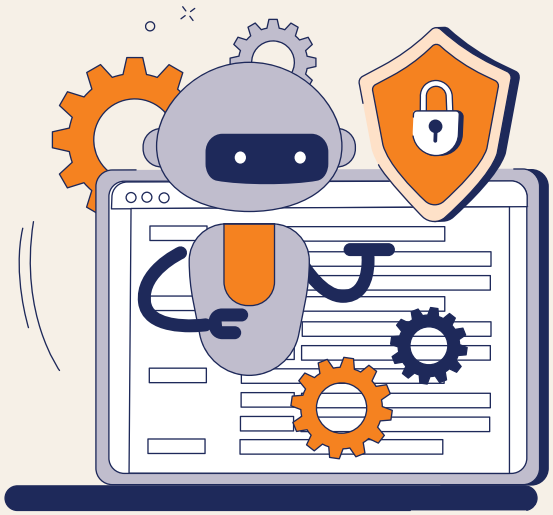
At this stage, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There may be an absence of observable evidence at this Stage.

Formative

Some features of the Aspect have begun to grow and be formulated but may be ad hoc, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated.

Established

The Indicators of the Aspect are in place, and evidence shows that they are working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the Aspect. However, the Aspect is functional and defined.



Dimension 1:

School cybersecurity policy and strategy

Dimension 1: School Cybersecurity Policy and Strategy

Factor 1.1: School Cybersecurity Policy

Aspect	Start-Up	Formative	Established
School Cybersecurity Strategy and Policy (Access and Adoption)	Policy does not exist or is not publicised when it does exist Cybersecurity strategy does not exist Lack of awareness about the need for a Cybersecurity Policy at Schools (SGB, SMT, ICT Committee) No resource (i.e. financial, equipment, human, etc.) is allocated towards cybersecurity in the school	An outline of cybersecurity strategy has been articulated The process for strategy development has been initiated School has access to cybersecurity policy template from PDE Most school SMT, SGB and educators are aware of the need for a cybersecurity policy Limited resources (i.e. financial, equipment, human, etc.) are allocated toward cybersecurity at the school	An approved cybersecurity strategy is available at school A school Cybersecurity strategy is implemented by stakeholders and promoted by SMT, SGB and Educators The school has adopted and implemented a cybersecurity policy based on the PDE template Significant resources (i.e. financial, equipment, human, etc.) are allocated toward cybersecurity at the school
Cybersecurity Content (In the cybersecurity policy or in any other relevant policies or as a rule at the school – With relevance to the Children's Act of 2005)	Cybersecurity content is lacking in other school policies (i.e. ICT, child protection, cybersecurity, etc.) School has contradictory cybersecurity rules (Counter cybersecurity rule) that create cybersecurity vulnerabilities School has unwritten rules that are cybersecurity relevant	Cybersecurity content is found in some school policies (i.e. ICT, child protection, Cybersecurity, etc.) Various strategies and policies relevant to cybersecurity do exist School acknowledges the existence of contradictory cybersecurity rules that create cybersecurity vulnerabilities	Cybersecurity content is found in most school policies and in its cybersecurity policy (i.e. ICT, child protection, Cybersecurity, etc.) Schools have mechanisms to mitigate the effect of contradictory cybersecurity rules
Implementation and review	No overarching cybersecurity implementation program has been developed	Cybersecurity strategy and policy implementation are being outlined and drafted Cybersecurity strategy and policy implementation schedule and resources are estimated Cybersecurity strategy and policy implementation program has commenced	The school has an approved cybersecurity strategy and policy implementation program Cybersecurity strategy and policy implementation program is completed Cybersecurity strategy and policy implementation program is marked for review

Aspect	Start-Up	Formative	Established
School Interprovincial and external stakeholder collaboration	There is no awareness of main national and international debates relating to school cybersecurity policy The school does not actively engage with potentially beneficial local, provincial and international networks and entities	There is limited awareness of main national and international debates relating to school cybersecurity policy The school has started to engage with potentially beneficial local, provincial and international networks and entities on cybersecurity	There is aware and contribute to main national and international debates relating to school cybersecurity policy School has cybersecurity metrics to measure capacity and document school-level incidents School has interprovincial and external stakeholder collaboration on cybersecurity

Factor 1.2: School Incident Response and Crisis Management

Aspect	Start-Up	Formative	Established
Identification and categorisation of incidents	No process/mechanism for identifying and categorising school-level incidents exists	A cybersecurity school level incident reporting form exist There is a list of cybersecurity events' categories as incident, emergency, and crisis held and maintained at the school	School has a process/mechanism to identify and categorise occurrences of school-level incidents
Organisation	No person or committee for school level incident response is dedicated or exists	School has appointed an Information Officer School has appointed an ICT committee	School has a cybersecurity committee
Integration of Cybersecurity into School Crisis Management	No framework exists for School-level crisis management Cybersecurity has not been considered a potential School-level crisis scenario Emergency communication capabilities are not clear	School has some emergency response mechanisms in place Cybersecurity is considered a potential School-level crisis scenario Emergency communication capabilities are available but limited	School has a cybersecurity crisis management framework School emergency communication capabilities can reach important stakeholders at any time Emergency communication capabilities are available and used to communicate on cybersecurity issues
Cyberbullying response	School is not engaging with school safety framework on cyberbullying School does not have access to verified DBE policy documents on cyberbullying School does not have access to cyberbullying response resources (i.e. Information, Social worker, SAPS school safety)	School has some awareness of but does not comply with the NDE policy on cyberbullying	School is compliant with the NDE policy on cyberbullying School has access to cyberbullying response resources (i.e. Information, Social workers, SAPS school safety)

Factor 1.3: School ICT infrastructure protection

Aspect	Start-Up	Formative	Established
Identification of ICT assets	There may be some appreciation of what constitutes an ICT asset, but no formal categorisation of ICT assets has been produced	There is a list of ICT assets at school	School has an inventory of ICT assets categorised per their importance
Regulatory Requirements	There are unwritten rules threatening the availability and the beneficial use of computers and the Internet There is no awareness of existing regulatory requirements or policies specific to the security of ICTs at school. (i.e. Laptop, USB, labs, admin office physical access, Internet access policies and etc)	School has identified unwritten rules threatening the availability and the beneficial use of computers and the Internet There is awareness of existing regulatory requirements or policies specific to the security of ICTs at school	School has mechanisms to identify and mitigate the effect of threatening unwritten rules on the availability and the beneficial use of computers and the Internet There is compliance with existing regulatory requirements or policies specific to the security of ICTs at school
Operational Practice	A few school ICT infrastructure users (i.e. ICT technicians, ICT committee, Educators, Administrative staff, SMT members, RCL/Prefects) may be implementing good cybersecurity practices, but this is inconsistent	Most school ICT infrastructure users implement good cybersecurity practices, but this is inconsistent	School ICT infrastructure users inconsistently implement good cybersecurity practices

Factor 1.4: Cybersecurity in School Security

Aspect	Start-Up	Formative	Established
Learners' safety co-ordination	School acknowledges the role of other entities or stakeholders in learners' safety, but relationships are not formalised for cybersecurity	Collaboration on cybersecurity amongst school stakeholders on learners' safety is limited	School stakeholders concerned with learners' safety formally collaborate on cybersecurity
School security cybersecurity capability	There is no access to or availability of specialist cybersecurity capability within the school security establishment	Access or availability of specialist cybersecurity capability within the school security establishment is limited	There is effective and regular access to or availability of specialist cybersecurity capability within the school security establishment

Dimension 2:

School cybersecurity culture

Dimension 2: School Cybersecurity Culture

Factor 2.1: Cybersecurity mindset

Aspect	Start-Up	Formative	Established
Awareness of cybersecurity threats and risks	The school has minimal or no level of awareness of cybersecurity threats and risks School external stakeholders have minimal or no level of awareness of cybersecurity threats and risks Users have minimal or no level of awareness of cybersecurity threats and risks	Most school stakeholders have a minimal level of awareness of cybersecurity threats and risks Some school external stakeholders have sufficient awareness of cybersecurity threats and risks Some users have sufficient awareness of cybersecurity threats and risks	Most school stakeholders have a medium level of awareness of with some stakeholders (SMT, SGB, ICT and Cybersecurity committee) with high level of awareness, knowledge and skills on cybersecurity threats and risks School external stakeholders have sufficient awareness of cybersecurity threats and risks Users have a sufficient level of awareness of cybersecurity threats and risks
School Management awareness raising	Awareness raising on cybersecurity issues for school management is non-existent School management are not yet aware of their responsibilities to Educators, parents, learners, administrative and ancillary staff in relation to cybersecurity awareness raising	Awareness raising on cybersecurity issues for school management is limited. School management have limited awareness of their responsibilities to Educators, parents, learners, administrative and ancillary staff in relation to cybersecurity awareness raising	Awareness raising on cybersecurity issues for school management is effective and regular School management have sufficient awareness of their responsibilities to Educators, parents, learners, administrative and ancillary staff in relation to cybersecurity awareness raising
School priority of cybersecurity	The school has minimal or no recognition of the need to prioritise cybersecurity School external stakeholders have minimal or no recognition of the need to prioritise cybersecurity Users have minimal or no recognition of the need to prioritise cybersecurity No surveys or metrics exist to document and measure cybersecurity in school	The school recognises the need to prioritise cybersecurity Some school external stakeholders recognise the need to prioritise cybersecurity Some users recognise the need to prioritise cybersecurity School recognises the need for surveys or metrics to document and measure some cybersecurity	The school prioritise of the need cybersecurity School external stakeholders recognise the need to prioritise cybersecurity Users recognise the need to prioritise cybersecurity School has surveys or metrics to document and measure cybersecurity

Aspect	Start-Up	Formative	Established
Cybersecurity Practice at School	The school does not follow safe cybersecurity Practices School external stakeholders do not follow safe cybersecurity Practices In this school, very few Internet users follow safe cybersecurity practices or take protective measures to ensure their security	The school follows basic safe cybersecurity Practices School external stakeholders follow basic safe cybersecurity Practices In this school, some Internet users follow safe cybersecurity practices or take protective measures to ensure their security	The school follows sufficient safe cybersecurity Practices School external stakeholders do follow safe cybersecurity Practices In this school, most Internet users follow safe cybersecurity practices or take protective measures to ensure their security

Factor 2.2 Trust and Confidence in Online Services and School Online Platforms

Aspect	Start-Up	Formative	Established
User Trust and confidence in online Search and information	Most school Internet users have no trust or have a blind trust in websites and what they see or receive online Very few school Internet users feel confident in performing online searches and in the quality of information from the Internet	Some school Internet users have informed trust in websites and what they see or receive online Some school Internet users feel confident in performing online searches and in the quality of information from the Internet	Most school Internet users have informed trust in websites and what they see or receive online Most school Internet users feel confident in performing online searches and in the quality of information from the Internet
User Trust in E-learning Services (i.e. LMS, Kahoot, Google classroom, Class Dojo)	School offers a very limited number of e-learning services, if any, and has not publicly promoted their security	School offers e-learning services but has not publicly promoted their security	School offers e-learning services and publicly promotes their security
User Trust in School administration online services (i.e. SASAMS, CEMIS, LURITS, Thutong portal, Provincial Online Admission platforms)	School users do not trust or trust a limited number of e-services offered by National and Provincial Governments Generally, school stakeholders (i.e. parents, learners, educators, SMT, SGB, SAPS, Health, Social service, etc.) do not use any significant School administration online services No surveys or metrics exist to show how school Internet users trust school administration online services There is a lack of information about School administration online services security and security breaches	Some school users trust a limited number of e-services offered by National and Provincial Governments Most school stakeholders (i.e. parents, learners, educators, SMT, SGB, SAPS, Health, Social service, etc.) use any significant School administration online service Some surveys or metrics exist to show how school internet users trust school administration online services There is limited information about School administration online services security and security breaches	School users trust e-services offered by National and Provincial Governments Generally, school stakeholders (i.e. parents, learners, educators, SMT, SGB, SAPS, Health, Social service, etc.) do not use any significant School administration online services Surveys or metrics exist to show how school Internet users trust school administration online services There is information about school administration online services security and security breaches

Aspect	Start-Up	Formative	Established
Disinformation Information verification skills to combat misinformation and disinformation (fake news)	National and provincial educational authorities' Internet platforms are not addressing issues of disinformation such as misinformation School external stakeholders (i.e. SAPS, social services, NGOs, community leadership, business entities, Health services, etc.) lack the tools and resources to address online disinformation, such as exposing misinformation Campaigns National and provincial educational authorities have not addressed online disinformation online.	National and provincial educational authorities' Internet platforms are addressing some issues of disinformation such as Misinformation School external stakeholders (i.e. SAPS, social services, NGOs, community leadership, business entities, Health services, etc.) have limited tools and resources to address online disinformation, such as exposing misinformation Campaigns National and provincial educational authorities have made efforts to address online disinformation online	National and provincial educational authorities' Internet platforms are addressing issues of disinformation such as Misinformation School external stakeholders (i.e. SAPS, social services, NGOs, community leadership, business entities, Health services, etc.) have the tools and resources to address online disinformation, such as exposing misinformation Campaigns National and provincial educational authorities have addressed online disinformation online
User Trust in E-commerce Services (i.e. online shopping, e-banking, etc.)	E-commerce services are not offered at school Internet users lack the trust to use any available school e-commerce services No surveys or metrics exist to show how Internet users trust school e-commerce services There is little or no recognition of the need for security initiatives for school e-commerce services	Some e-commerce services are offered at school Most internet users trust to use any available school e-commerce services Some surveys or metrics exist to show how Internet users trust school e-commerce services School recognises the need for security initiatives for school e-commerce services	E-commerce services are offered at school Internet users trust school e-commerce services Surveys or metrics exist to show how Internet users trust school e-commerce services There is recognition of the need for security initiatives for school e-commerce services

Factor 2.3 School stakeholders' understanding of personal information protection Online

Aspect	Start-Up	Formative	Established
Personal information protection online	Users and stakeholders within the school context have no or minimal knowledge about how personal information is handled online, nor do they believe that adequate measures are in place to protect their personal information online There is no or limited discussion regarding the protection of personal information online at school Privacy standards are not in place to shape Internet and social media practices at school	Most users and stakeholders within the school context have knowledge about how personal information is handled online and believe that adequate measures are in place to protect their personal information online There is limited discussion regarding the protection of personal information online at school There are some privacy standards in place to shape Internet and social media practices at school	Users and stakeholders within the school context have knowledge about how personal information is handled online, and adequate measures are in place to protect their personal information online There are discussions regarding the protection of personal information online at school Privacy standards are in place to shape Internet and social media practices at school

Factor 2.4 Reporting Mechanism (Whistle Blowing)

Aspect	Start-Up	Formative	Established
Reporting mechanism	There are no official reporting mechanisms available, but discussions might have begun at school School stakeholders do not use social media channels to raise concerns over any cyber harms and problems No metrics of reported incidents exist	There are some official reporting mechanisms available, but discussion have begun at school Some school stakeholders use social media channels to raise concerns over any cyber harms and problems Some metrics of reported incidents exist	There are official reporting mechanisms in the school School stakeholders use social media channels to raise concerns over any cyber harms and problems School has metrics of reported incidents exist

Factor 2.5 Social Media and School Online Platforms

Aspect	Start-Up	Formative	Established
Social Media and School online platforms (i.e., LMS, social media, email, virtual meeting platforms, Zoom, Teams, remote learning)	School communications rarely, if ever, cover information about cybersecurity or report on issues such as security breaches or cybercrime There is no, or rarely any discussion on social media or newsletters about Cybersecurity Any portrayal of whistleblowers is negative and based on negative stereotypes	School communications sometimes cover information about cybersecurity or report on issues such as security breaches or cybercrime Sometimes there are discussions on social media or newsletters about Cybersecurity Whistleblowers are accepted, although they are sometimes hampered by negative stereotypes	School communications information about cybersecurity or report on issues such as security breaches or cybercrime There are discussions on social media or newsletters about Cybersecurity Whistleblowers are positively received

Dimension 3:

School cybersecurity training and skills

Dimension 3: School Cybersecurity Training and Skills

Factor 3.1: Cybersecurity training

Aspect	Start-Up	Formative	Established
Cybersecurity Training provision (certification)	Few or no training programmes in cybersecurity exist	Few training programmes in cybersecurity exist	Training programmes in cybersecurity exist
Cybersecurity Training uptake	Training uptake by personnel (ICT educators, Cybersecurity committee, SGB, SMTs and admin staff) designated to respond to cybersecurity incidents is limited or non-existent There is no transfer of knowledge from employees trained in cybersecurity to untrained employees	Some school stakeholders, take up training to respond to cybersecurity incidents is limited or non-existent There is a reasonable transfer of knowledge from employees trained in cybersecurity to untrained employees	Training uptake by personnel (ICT educators, Cybersecurity committee, SGB, SMTs and admin staff) designated to respond to cybersecurity incidents is limited or non-existent There is a transfer of knowledge from employees trained in cybersecurity to untrained employees

Factor 3.2: Digital literacy and cybersecurity skills

Aspect	Start-Up	Formative	Established
Digital Literacy skills	Limited digital literacy is available among school stakeholders	Most school stakeholders have digital literacy skills	School stakeholders have digital literacy
Cybersecurity skills	Limited cybersecurity skills are available among school stakeholders Limited access to a person with professional cybersecurity skills and competencies	Most school stakeholders have cybersecurity skills Reasonable access to a person with professional cybersecurity skills and competencies	School stakeholders have cybersecurity skills Unlimited access to a person with professional cybersecurity skills and competencies

Dimension 4:

School cybersecurity legal and regulatory compliance

Dimension 4: School Cybersecurity Legal and Regulatory Compliance

Factor 4.1: Policy and regulatory requirements

Aspect	Start-Up	Formative	Established
Cybersecurity Policies for Schools	Access to cybersecurity policies does not exist General ICT/ cybersecurity rules may exist, but their application to cybersecurity is unclear	School recognises the need for cybersecurity policies School has developed a cybersecurity implementation plan There are cybersecurity policy requirements complied with such as cyberbullying policy	School has access to cybersecurity policies General ICT/ cybersecurity rules exist, and application to cybersecurity is clear School has implemented its cybersecurity policy
School legal and regulatory requirements for cybersecurity	There is no awareness of legal and regulatory frameworks (stakeholders in the school) There is limited compliance with school cybersecurity requirements set out in regulations or laws The need to comply with regulatory frameworks on school cybersecurity may have been recognised and may have resulted in a gap analysis	School management is aware of some legal and regulatory frameworks The school recognises all cybersecurity requirements set out in regulation or law Some general ICT/ cybersecurity rules exist, and their application to cybersecurity is clear School complies with most requirements of the cybersecurity policy	All school stakeholders are aware of legal and regulatory frameworks School complies with all cybersecurity requirements set out in regulations or laws (POPI, PAIA, ECTA and Cybercrime acts) The school has a regulatory framework on cybersecurity School has a cybersecurity officer and a committee School has cybersecurity compliance metrics at school
School cybersecurity legislation and regulation compliance officer	There is no appointed cybersecurity officer or committee at school There are no cybersecurity compliance metrics at school	School recognises the need for a cybersecurity officer or committee at school There are partial cybersecurity compliance metrics at school	School has appointed a cybersecurity officer or committee School has adopted or developed cybersecurity compliance metrics

Factor 4.2: Related policy frameworks

Aspect	Start-Up	Formative	Established
Data Protection Policy (Provincial/ National Department of Education (PDE/ DBE)	PDE/DBE Data protection policy template for school does not exist There is little or no awareness of cybersecurity policy and regulatory frameworks (stakeholders in the school)	School has access to the data protection policy Most school stakeholders are aware of cybersecurity policy and regulatory frameworks	School complies with data protection policy School stakeholders are aware There of policy and regulatory frameworks
Child Protection Online (i.e. Relevance to Children's Act of 2005)	School policies relating to child protection is limited, and their application in the online environment is yet to be considered	School recognises most policies relating to child protection in online Environment	School adheres to policies relating to child protection in the online environment
Intellectual property policies	National and PDE policies related to intellectual property protection is limited and its application in the online environment is yet to be considered	School recognises National and PDE policies related to intellectual property protection but does not fully comply with it in online environments	National and PDE policies related to intellectual property protection is clear and fully applied in online environments
Data protection and privacy legislation	Awareness of Data protection and Privacy legislation (ECTA, POPI, PAIA) is limited There is no compliance with Data protection and privacy legislation (ECTA, POPI, PAIA)	Most school stakeholders are aware of Data protection and Privacy legislation (ECTA, POPI, PAIA) School complies with some sections of Data protection and privacy legislation (ECTA, POPI, PAIA)	School stakeholders are aware of Data Protection and Privacy legislation (POPI, PAIA) is limited School complies with Data protection and privacy legislation (ECTA, POPI, PAIA) School has measures to assess its compliance with Data protection and privacy legislation

Factor 4.3: Co-operation Frameworks to Combat Cybercrime at schools

Aspect	Start-Up	Formative	Established
Law Enforcement Co-operation with schools	Co-operation between school and law enforcement has not been established	School recognises the need to co-operate with law enforcement and sometimes consult with them on cybersecurity issues	School has established formal and informal collaboration and co-operation with law enforcement
Social services cooperation with schools	Co-operation between school and social services to combat cybercrime has not been established	School recognises the need to co-operate with social services and sometimes consult with them on cybersecurity issues	School has established formal and informal collaboration and co-operation with social services
Community leadership (i.e. Religious, traditional, political and neighbourhood) cooperation with schools	Co-operation between school and community leadership to combat cybercrime has not been established	School recognises the need to co-operate with community leadership and sometimes consult with them on cybersecurity issues	School has established formal and informal collaboration and co-operation with community leadership

Dimension 5:

School cybersecurity legal and regulatory compliance

Dimension 5: School Cybersecurity Standards and Technologies

Factor 5.1: Adherence to DBE/PDE cybersecurity standards for schools

Aspect	Start-Up	Formative	Established
ICT security standards and best practices	No standards or best practices have been identified for use in securing data, technology or infrastructure by the school PDE/DBE does not suggest basic cybersecurity standards or practices for schools	School applies basic cybersecurity standards or practices in securing data, technology or infrastructure by the school PDE/DBE has established and communicated cybersecurity standards and best practices for schools School is aware of PDE/DBE cybersecurity standards and best practices for schools	School adheres to standards and best practices in securing data, technology or infrastructure established by the PDE/DBE School has developed metrics or mechanisms to assess adherence to cybersecurity standards and best practices

Factor 5.2: Security Controls

Aspect	Start-Up	Formative	Established
Technological Security controls	There is minimal or no understanding or deployment of the technological security controls available in the marketplace by school stakeholders (e.g. anti-virus, firewall, Biometric/card/token/challenge access control systems, physical security)	Some school stakeholders have knowledge and understanding or deployment of the technological security controls available in the marketplace by s (e.g. anti-virus, firewall, biometric/card/token/challenge access control systems, physical security) Some technological security controls are implemented at the school	School stakeholders have knowledge and understanding or deployment of the technological security controls available in the marketplace by s (e.g. anti-virus, firewall, Biometric/card/token/challenge access control systems, physical security) School has implemented the PDE/ DBE suggested standards for school technological security controls
Physical Security of Laptops / Desktops	School does not implement basic physical security control measures such as Locked door policy, Security gates, burglar bars, privileged access, fire detection and suppression, backup power supply, CCTV, Alarms, or security guards School does not implement best practices in users' authentication on laptops and desktops (i.e. regular password update, multifactor authentication, tokens or PIN) School does not have an inventory of ICT assets SGB does not provide means (i.e. technicians, insurance, and other security features) to secure School ICT assets	School has implemented some basic building safety and facility security controls including two or more of the following: gates and fences, fire detection and suppression, backup power supply, CCTV, Alarms, or security guards School implements passwords, tokens, PIN or multifactor authentication on laptops and desktops School has an inventory of ICT assets SGB contributes to accessing one or more of the following means to secure School ICT assets: cyber technician, insurance, and other security features	School implements basic building safety and facility security controls School implements best practices in computer facility access controls. School has an ICT assets inventory management system SGB provide further means (i.e. technicians, insurance, and other security features) to secure School ICT assets

Aspect	Start-Up	Formative	Established
Cryptographic Controls for schools (document encryption, electronic signature, communication tunnelling – Virtual Private Network)	Cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and data in transit may be a concern but are not yet deployed within the school School is not aware of PDE/DBE standards and use of cryptographic techniques for schools PDE/DBE does not have standards for the use of cryptographic techniques for schools PDE/DBE does not deploy cryptographic techniques for schools	Some school stakeholders are aware of the cryptographic techniques (e.g. encryption and digital signatures) for the protection of data at rest and data in transit PDE/DBE has established standards for the use of cryptographic techniques for schools PDE/DBE deploys cryptographic techniques for schools for the protection of data at rest and data in transit	Cryptographic techniques (e.g. encryption and digital signatures) for the protection of data at rest and data in transit have been deployed within the school School stakeholders are aware of PDE/DBE standards for the use of cryptographic techniques (e.g. encryption and digital signatures) to protect data at rest and data in transit

Factor 5.3: Software Quality and Internet Infrastructure Resilience

Aspect	Start-Up	Formative	Established
Software Quality and Assurance	Quality and performance of software used in the school is a concern, but functional requirements are not yet fully monitored A catalogue of assured software platforms and applications within the school (i.e. provided by PDE/DBE) does not exist Policies and processes regarding updates and maintenance (including patch management) of software applications have not yet been formulated (i.e. Provided by PDE/DBE)	School has acceptable quality software however performance of software used in the school is a concern, but functional requirements are moderately monitored A catalogue of assured software platforms and applications for the school (i.e. provided by PDE/DBE) is available Some policies and processes regarding updates and maintenance (including patch management) of software applications have been formulated (i.e. Provided by PDE/DBE)	School has good quality software with good performance and functional requirements are fully monitored A school catalogue of assured software platforms and applications (i.e. provided by PDE/DBE) is available and used by school stakeholders Policies and processes regarding updates and maintenance (including patch management) of software applications have been formulated (i.e. Provided by PDE/DBE)
Internet Infrastructure Reliability	Affordable and reliable Internet services and infrastructure in the school may not have been established; if they have been, adoption rates of those services are a concern Network redundancy measures may be considered, but not in a systematic, comprehensive fashion Electricity supply is erratic	Affordable Internet services and infrastructure in the school may have been established; but adoption rates of those services are a concern Network redundancy measures are in place, but not in a systematic, comprehensive fashion School has a continuous electricity supply	Affordable and reliable Internet services and infrastructure in the school have been established; with high, adoption rates of those services among school stakeholders Network redundancy measures are considered, in a systematic, comprehensive fashion School has a redundant and continuous electricity supply

Bibliography

Global Cyber Security Capacity Centre (2021) Cybersecurity Maturity Model for Nations, GCSCC

Government of South Africa. (2015). South African government gazette: National cybersecurity policy Framework. https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000#

Acknowledgements

The CY4MAS was developed by C3SA with significant contributions from:

National Research Foundation (South Africa)

Western Cape Education Department

Limpopo Department of Education

Department of Information Systems - University of Cape Town

Department of Education Studies - University of Limpopo

Global Cyber Security Capacity Centre

South African Police Service

Schools that participated in the project:

- Citrusdal Primary School
- Sinenjongo Secondary School
- Thogoa Secondary School
- Ditlalemeso Secondary School
- Diphuti Primary School
- Emil Weder Secondary School
- Dunoon Primary School
- Good Hope Primary School

Project Team

Principal Investigators:

Prof Chigona, Wallace

Prof Mabasa, Layane Thomas

Lead Researchers:

Bagui, Laban (PhD)

Magunje, Caroline (PhD)

Researchers:

Calandro, Enrico (PhD)

Chimboza, Tendani (PhD)

Lusinga, Shallen (PhD)

Mabhena, Zwelithini

Makofane, Baby Inneth (PhD)

Mathiba, Thema Adolph (PhD)

Mphasha, Elisa Sebina

Mphahlele, Leswene

Mtegha, Chimwemwe

Pule, Nthabiseng

Ruhwanya, Zainab

Seshoka, Matome Winter (PhD)

Sowon, Karen (PhD)

Tuyeni, Teofelus

Research assistants:

Alagha, Ihab

Benjamin, Naseera

Du Plessis, Carlo S.

Kahn, Saajida

Kautondokwa, Popyeni

Mohlala, Aletta

Kleinbooi, Thapedi Selowa

Rakgoroana, Sheila Elinah

Sabuka, Zibele Monwabisi

Cybersecurity Champions at schools:

Anders, Cherylene

Chirova, David

Cyster, Cyril

De Jager, Wayne

Makhafole, Tebogo Klaas

Sekgobela, Malesela Phineas

Zulu, Luvuyo

About the C3SA

The Cybersecurity Capacity Centre for Southern Africa (C3SA) is a consortium between Research ICT Africa (RIA), the Department of Information Systems (DIS) at the University of Cape Town (UCT), the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, and the Norwegian Institute of International Affairs (NUPI).

C3SA is part of the global constellation of regional cybersecurity capacity research centres which includes the Global Cyber Security Capacity Centre (GCSCC) and Oceania Cyber Security Centre (OCSC).

C3SA

Cybersecurity Capacity Centre for Southern Africa

Cybersecurity Capacity Centre for Southern Africa (C3SA)
Department of Information Systems | University of Cape Town
Commerce Building | Upper Campus
Private Bag X3
Rondebosch 7701
Cape Town
South Africa

Tel: +27 (0) 21 650 2261
Email: C3sa@uct.ac.za
Web: https://c3sa.uct.ac.za/

April 2025