



Resilio Africa Program Brief



Table of Content

Introduction	1
What Are Critical Community Institutions (CCIs)?	1
Why CCIs Matter and the Cyber Threats They Face	2
Common Threats Facing CCIs	2
Why Protecting CCIs Is Critical	3
Program Overview	3
Who Resilio Africa Supports	4
Get Involved	5

Introduction

Across Sub-Saharan Africa, Critical Community Institutions (CCIs) are increasingly targeted by cyberattacks. These organizations collect, process, and store vast volumes of sensitive personal and operational data, yet most lack the cybersecurity maturity required to protect it. Many operate on outdated systems, with limited technical capacity, low awareness of digital threats, and little to no dedicated security budgets.

Regional data highlights the scale of the challenge. Africa experienced a 23 percent increase in ransomware attacks in 2023, with public and nonprofit institutions among the most impacted¹. At the same time, more than 60 percent of African countries fall within the “low commitment” category for national cybersecurity readiness². This systemic gap leaves community-level institutions particularly exposed as essential services continue to digitize.

For CCIs, cyber incidents are not abstract technical events. They directly disrupt healthcare delivery, education, access to public services, and trusted community information. As attackers increasingly target organizations perceived as high-impact but low-resilience, the need for practical, accessible cybersecurity support at the community level has become urgent.

What Are Critical Community Institutions (CCIs)?

Critical Community Institutions are organizations whose primary role is to sustain community well-being, inclusion, and resilience at the local or regional level. They may be publicly owned, nonprofit, cooperative, or community-focused private entities.

What defines a CCI is not ownership but function and impact.

CCIs share these defining characteristics:

- Deliver essential public-facing services, rather than prioritizing profit.
- Serve large populations or vulnerable groups at the community level
- Manage sensitive citizen, health, education, or service-delivery data
- Operate close to the people they serve, where service disruptions have immediate human impact

This functional definition captures a wide range of institutions that quietly underpin everyday life across Sub-Saharan Africa.

¹ INTERPOL. (2024). INTERPOL African Cyberthreat Assessment Report 2024.

[https://www.interpol.int/content/download/21048/file/24COM005030-](https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf)

[AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf](https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf)

² Telecommunication Union. (2021). Global Cybersecurity Index (GCI) 2020. ITU. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

Why CCIs Matter and the Cyber Threats They Face

Communities rely on far more than national infrastructure to function. Local hospitals and clinics, schools, municipal offices, water and sanitation services, ICT hubs, community media houses, and cooperative institutions provide the services people interact with most frequently.

When these institutions are disrupted by cyber incidents, the effects are immediate:

- A ransomware attack on a clinic can delay or deny patient care
- A data breach at a local council can expose thousands of citizen records
- A denial-of-service attack on a school or community media platform can cut off access to education or trusted information

Because CCIs operate closest to the people they serve, cyber incidents at this level often have a more visible and human impact than failures in national systems.

Common Threats Facing CCIs

CCIs are increasingly targeted by cybercriminals because they are both high-impact and low-resilience targets.

Common threats include:

- Ransomware attacks aimed at quick financial gain
- Phishing and credential theft exploiting low awareness
- Data breaches exposing sensitive personal and institutional information
- Service disruption attacks targeting public-facing systems

These threats are amplified because many CCIs:

- Operate outdated or unpatched systems
- Lack dedicated cybersecurity staff or budgets
- Have limited access to incident response or threat intelligence support

Recent data illustrates this exposure. In Kenya alone, more than 114 cyberattacks targeting critical community infrastructure were recorded in the first eight months of 2024³, followed by a 201 percent increase in detected cyber incidents by the first quarter of 2025⁴. Similar patterns are observed across Nigeria, Ghana, and South Africa, where many public-serving institutions continue to operate without baseline security controls.

³ Top Tech (2024). Kenya Recorded 114 Cyber-Attacks on Critical Infrastructure in 2024. <https://toptechgh.com/kenya-recorded-114-cyber-attacks-critical-infrastructure-2024/>

⁴ Top Tech (2025). Kenya Detected 2.5 Billion Cyber Threats in Q1 2025. <https://toptechgh.com/kenya-detected-2-5-billion-cyber-threats-in-q1-2025/>

Why Protecting CCIs Is Critical

Cybersecurity incidents affecting CCIs extend beyond systems and data. They disrupt essential services, erode public trust, and place already vulnerable communities at greater risk.

Despite growing national attention to cybersecurity, most CCIs remain under-resourced and under-protected. Without scalable, context-aware interventions designed specifically for community institutions, cyber risks will continue to outpace defensive capacity.

Resilio Africa was established to close this protection gap by providing practical, accessible, and context-aware cybersecurity support tailored specifically to the realities of Critical Community Institutions across Sub-Saharan Africa.

Program Overview

Resilio Africa is designed for institutions that cannot afford to fail but also cannot sustain a complex or expensive cybersecurity program.

The program supports resource-constrained CCIs through practical risk reduction, capacity building, and long-term resilience. It prioritizes actionable security improvements over heavy compliance requirements or costly tooling. Resilio Africa meets CCIs where they are and strengthens their ability to protect the communities they serve.

Participation in Resilio Africa is fully subsidized for selected institutions.

What Resilio Africa Provides



Security Health Check

Comprehensive cybersecurity maturity assessments, risk profiling, and gap analysis, followed by clear, prioritized recommendations.



Capacity Building and Training

Targeted training for leadership, IT teams, and general staff to strengthen governance, awareness, and everyday security practices.



Threat Intelligence and Exposure Monitoring

Access to curated threat intelligence and monitoring tools to identify emerging risks and exposed assets.



Phishing Simulations and Readiness Exercises

Realistic simulations and tabletop exercises to test preparedness and strengthen response capabilities.



Incident Response Playbooks and Support

Customized response playbooks, implementation guidance, and technical support to reduce response time and impact during incidents.



Expert Consultations

Direct access to cybersecurity specialists for policy development, control implementation, and ongoing security decision-making.



Regional Cyber Defense Network

Integration into a trusted regional network of CCIs and technical partners for information-sharing, coordination, and collective resilience.

By combining human, procedural, and technical elements, Resilio Africa strengthens the ability of CCIs to prevent, detect, and respond to cyber threats.

Over the life of the program, Resilio Africa will support 200 CCIs, help protect services relied upon by over 2 million people, and secure more than 15 million public records across Nigeria, Kenya, Ghana, and South Africa.



Resilio Africa is delivered by CyberSafe Foundation with support from [Google.org](https://www.google.org)

Who Resilio Africa Supports

Eligibility Criteria

To participate in Resilio Africa, organizations must:

- Be formally registered in Nigeria, Kenya, Ghana, or South Africa
- Belong to one of the approved CCI functional categories

Resilio Africa works with Critical Community Institutions across four key functional categories:

Category	Examples
Educational, environmental, and local services	Schools, community colleges, special education providers, libraries, ICT hubs, parks and recreation facilities, municipal or cooperative housing, residents' associations, town planning and traffic management offices, volunteer fire brigades, first aid groups, disaster response NGOs, civil protection volunteers, and employment or job centers, etc.
Health, sport, and care organizations	Hospitals, clinics, laboratories, water and sanitation boards, sports clubs and facilities, shelters, refuges, food banks, care homes, crisis helplines, therapy and listening services, adoption services, and early childhood care providers, etc.
Cultural and creative organizations	Theatres, museums, dance studios, music groups, youth clubs, local newspapers and radio stations, arts centres, faith-based community projects, etc.
Public Administration Systems	Municipal offices, local government authorities, and select government ministries, departments, and agencies.

Get Involved

If your organization provides essential services to communities and wants to strengthen its cybersecurity resilience, Resilio Africa is here to support you. Participation is **completely free**. No fees or financial contributions are required from selected institutions.

Apply to participate or learn more: www.resilio.cybersafefoundation.org

For inquiries, contact: resilio@cybersafefoundation.org

Delivered by CyberSafe Foundation

CyberSafe Foundation is a nonprofit advancing cybersecurity and AI inclusion across Africa, focusing on underserved communities. With programs in 27+ African Countries, we have reached over 200 million people and supported governments, schools, nonprofits, and critical community institutions with practical, context-aware interventions.

Learn More: www.cybersafefoundation.org



Connect With Us

Email: resilio@cybersafefoundation.org

Instagram: <https://instagram.com/cybersafehq>

Twitter: <https://twitter.com/cybersafehq>

LinkedIn: <https://linkedin.com/company/cybersafefoundation>

Facebook: <https://facebook.com/cybersafefoundation>

Website: www.resilio.cybersafefoundation.org

Written and Designed by Success Tawo

