

Authors:

Elizabeth Kolade
Adeboro Odunlami
Nanbaan Pwaspo
Abigail Ebiware

Design & Layout:

Ibrahim Gambo

Illustration:

Tiolu Yoloye

Copyright © 2024 Resilience Technologies

This publication may be reproduced for non-commercial use in any form provided due credit is given to the publishers, and the work is presented without any distortion.

Table of Content

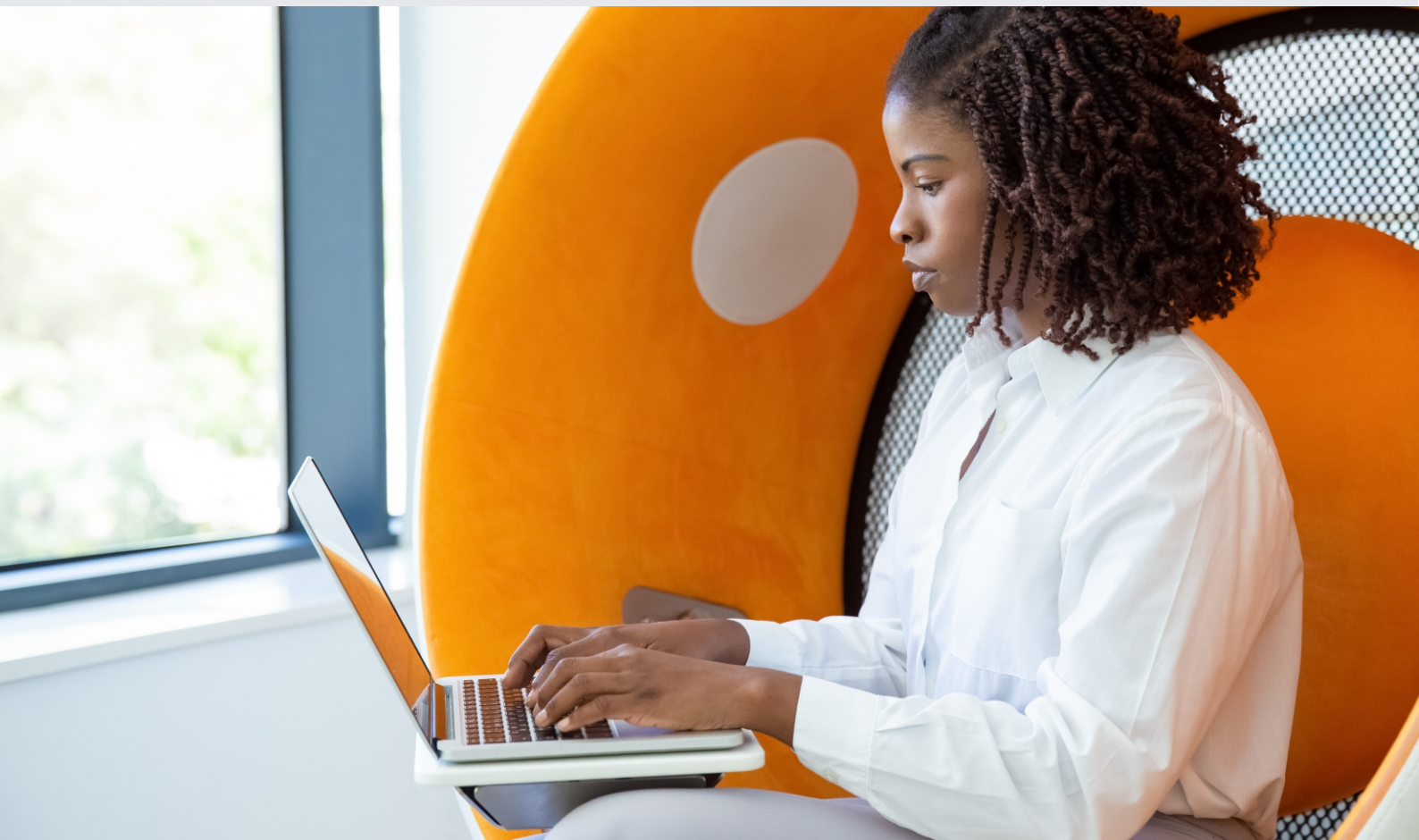
0.0 Executive Summary	Page 1
1.0 Introduction	Page 2
2.0 About Resilience Technologies	Page 5
3.0 Methodology	Page 6
4.0 State of Digital Security	Page 8
5.0 Identified Risks and Vulnerabilities	Page 19
6.0 The Resilience Design Intervention	Page 20
7.0 Findings	Page 22
8.0 Challenges	Page 24
9.0 The Resilience Model	Page 26
10.0 Conclusion	Page 29

Executive Summary

In response to the growing importance of digital security for CSOs and at-risk communities in Africa, this comprehensive report details the findings of Resilience Technologies's RT-10 digital security assessment project. The findings and recommendations presented herein are the result of a detailed assessment conducted across a diverse array of CSOs, revealing both strengths and vulnerabilities in their digital security postures. The report begins by providing context on the methodology explored in carrying out this assessment via a focus group. It, then, details the state of digital security under the headings of people, processes, technology, and policies.

The findings reveal a deficiency in digital security awareness among staff, emphasising the need for comprehensive and continuous training. Risk factors, particularly at the leadership level, underscore the significance of targeted security measures. Processes related to access control and data management exhibit inconsistencies, exposing organisations to potential breaches. There is a significant absence of comprehensive digital security policies in these organisations, which leads to inconsistencies in their digital security practices. The report concludes by presenting recommendations to CSOs, funders, and digital security organisations, as well as opportunities for further research.





1.0 Introduction

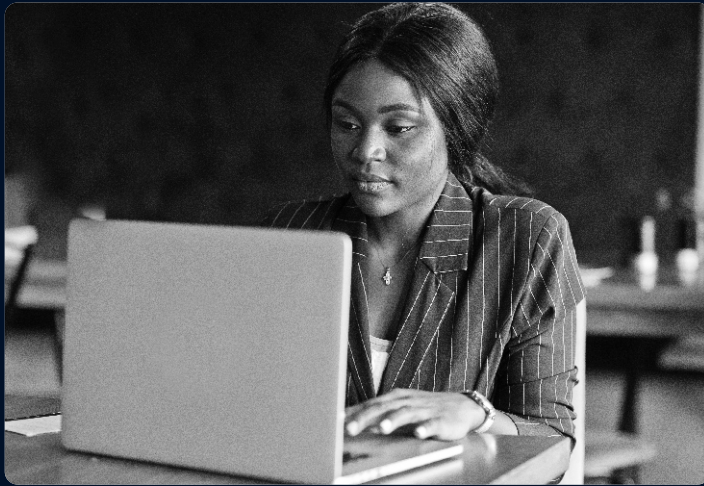
The importance of a robust digital resilience plan for civil society organisations (CSOs) and groups cannot be overstated. Especially in light of the increasing reliance of organisations on digital technologies and the reality of targeted digital attacks, building digital resilience has become a core necessity for CSOs to successfully carry on their work.

In recognition of the critical role they play and the risks they face, Resilience Technologies embarked on the RT-10 project, a programme aimed at understanding how CSOs in sub-Saharan Africa approach digital resilience and the security practices that underlie .

The result is a series of comprehensive digital resilience support to each of the ten selected organisations of the programme, and this report highlights important findings of their practices and recommendations to the broader civil society and digital security community.

1.0 Introduction

RT-10 also presented us with an opportunity to assess the viability of our Resilience Model, a rapid yet long-term and holistic approach to building digital resilience within civil society organisations, using this focus group of organisations. From pre-assessment to the deployment of recommendations, each solution within the resilience model was tested with observations to improve the model.



The importance of a robust digital resilience plan for civil society organisations (CSOs) and groups cannot be overstated. Especially in light of the increasing reliance of organisations on digital technologies and the reality of targeted digital attacks, building digital resilience has become a core necessity for CSOs to successfully carry on their work.

In recognition of the critical role they play and the risks they face, Resilience Technologies embarked on the RT-10 project, a programme aimed at understanding how CSOs in sub-Saharan Africa approach digital resilience and the security practices that underlie. The result is a series of comprehensive digital resilience support to each of the ten selected organisations of the programme, and this report highlights important findings of their practices and recommendations to the broader civil society and digital security community.

RT-10 also presented us with an opportunity to assess the viability of our Resilience Model, a rapid yet long-term and holistic approach to building digital resilience within civil society organisations, using this focus group of organisations. From preassessment to the deployment of recommendations, each

“

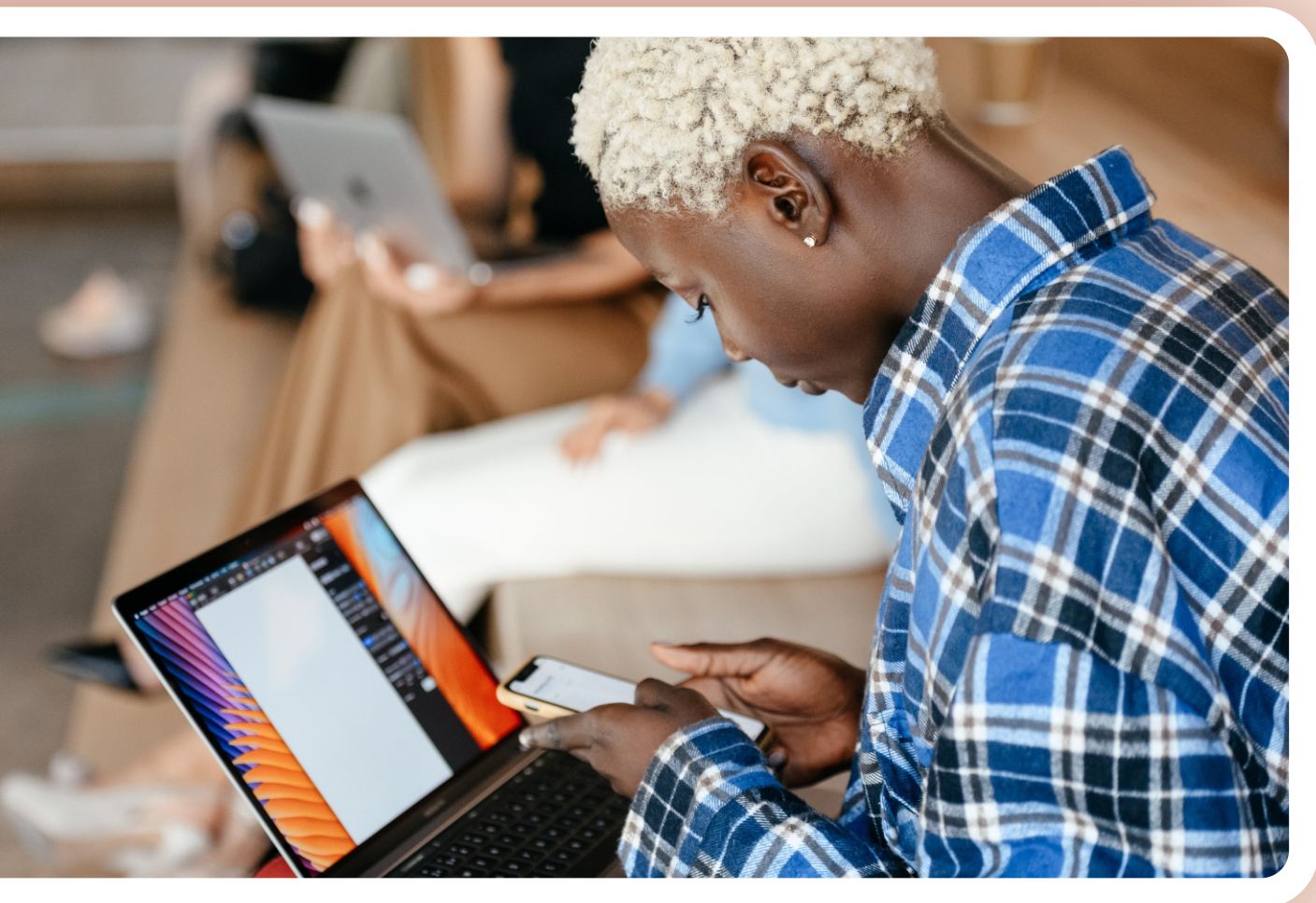
The Resilience Model isn't just a concept; it's a tested and proven approach, serving as a robust framework for enhancing digital defences within civil society organisations and beyond.

”

solution within the resilience model was tested with observations to improve the model.

By conducting this assessment, we aspired to primarily provide actionable insights and recommendations to empower the CSOs that were assessed and to fortify their digital defences, enabling them to focus on their core missions without compromising the security of their operations or the sensitive information they handle. In a broader sense, our goal with this assessment was to help the community of rapid responders and cybersecurity professionals in the internet freedom space understand just the kind of solution to deploy, at what level of effort, and for which types of organisations, especially for the African CSO.

The ensuing report encapsulates the collective findings of this assessment, delving into the specific nuances and challenges encountered during the program. It offers an understanding of the digital security landscape for CSOs in Sub-Saharan Africa, with a view to fostering a safer digital environment that amplifies the positive impact of these organisations.





2.0 About Resilience Technologies

Resilience Technologies is a non-profit organisation committed to providing research-driven and innovative digital security support and services to civil society and at-risk communities in Africa. At the core of our work is protecting and building the digital resilience of civil society organisations in Africa, as they rely on digital technologies to carry on their work of promoting democratic principles and defending the defenceless.

3.0 Methodology

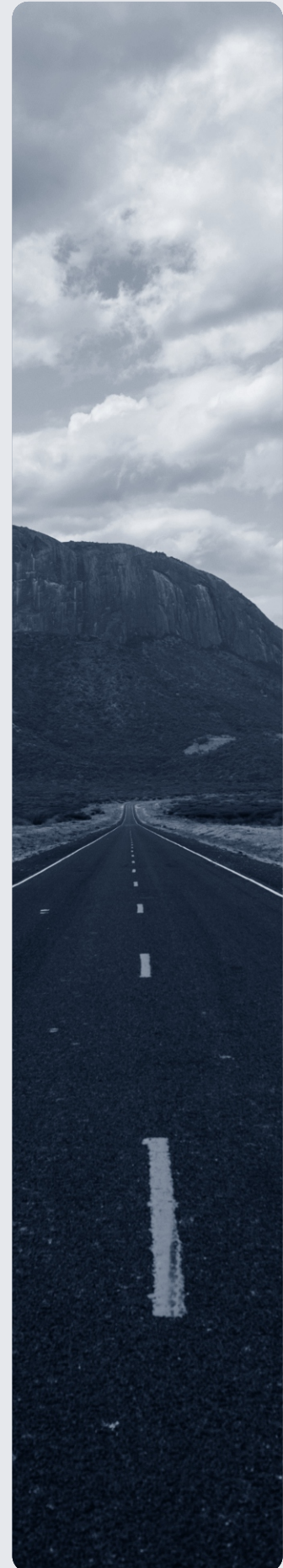
In conducting these assessments, we engaged in a multifaceted process designed to carefully select and comprehensively evaluate the digital security posture of civil society organisations (CSOs) within the focus group. The methodology consisted of the following key stages:

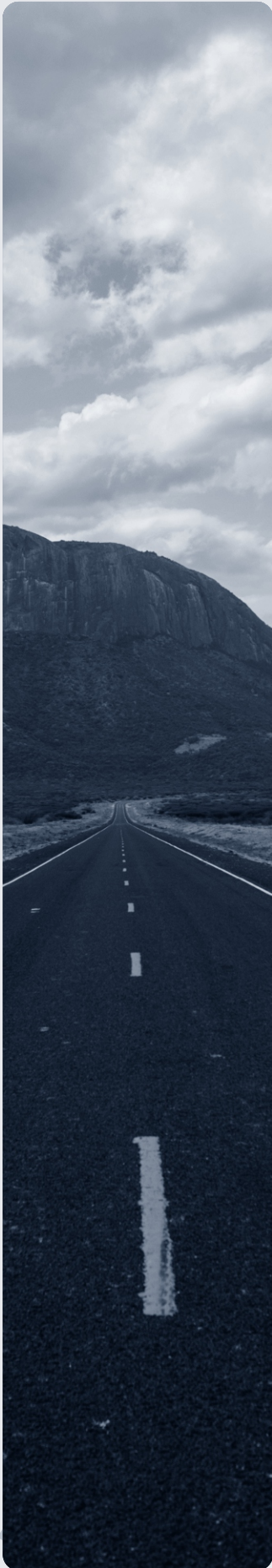
A. Pre-Assessment and Selection

We published and disseminated an open call for CSOs across Sub-Saharan Africa to apply to join the program. After a sufficient period, we conducted an initial pre-assessment of all 21 applicant organisations across Africa and selected 10 (eventually working with 8) whose work span across Uganda, Zimbabwe, Kenya, Nigeria, Ethiopia, and Tanzania. For selection, we utilised a set of criteria focused on notable digital security gaps, including a history of security incidents, targeted harassment, and an absence of prior security assessments or interventions.

B. Tool and Framework Selection

We deployed a combination of established tools and frameworks for the assessment process, such as the Digital Wellness Check (DWC) tool by the Centre for Digital Resilience, Penetration Testing and Vulnerability Assessment, NIST Standard Pentesting and OWASP testing tools to identify vulnerabilities, Jigsaw, OpenDNS, Phishingbox Quiz to assess and enhance security measures, and the Resilience Technology Security Assessment Framework.





C. Onboarding and Assessment Process

We deployed a combination of established tools and frameworks for the assessment process, such as the Digital Wellness Check (DWC) tool by the Centre for Digital Resilience, Penetration Testing and Vulnerability Assessment, NIST Standard Pentesting and OWASP testing tools to identify vulnerabilities, Jigsaw, OpenDNS, Phishingbox Quiz to assess and enhance security measures, and the Resilience Technology Security Assessment Framework.

D. Assessment Report and Interaction

Upon completion of the assessment, each organisation received a comprehensive DWC Report and Website Security Review Report outlining the findings of our assessment, after which we engaged with each organisation to discuss the assessment report and recommendations. We also conducted a Policy and Resilience Plan chat with each organisation to address internal digital security policy gaps. Finally, we offered the organisation free remediation for identified vulnerabilities.

E. The Resilience Design

In line with the goals of the assessment, we presented a tailored resilience plan in line with our “Resilience Design” to each organisation, incorporating actionable steps to improve digital and operational security and resilience.

Methodology



4.0 State of Digital Security

In conducting these assessments, we engaged in a multifaceted process designed to carefully select and comprehensively evaluate the digital security posture of civil society organisations (CSOs) within the focus group. The methodology consisted of the following key stages:

A. People

Highly underestimated and yet critically potent is the human factor in a large percentage of data and security breaches. People are often the most common vector used to attack organisations and it is no different within Civil Society Organisations and at-risk communities.

“

While many CSOs in Africa boast industry experts and activists among their ranks, the RT-10 assessment reveals a critical gap in digital security knowledge, underscoring the need for comprehensive training to mitigate inherent risks.

”

The RT-10 assessment revealed that although many CSOs in Africa are often made up of expert industry leaders and activists, only a few are truly equipped to understand basic and intricate aspects of digital security and this contributes a layer of risk to an already risk-prone organisation.

CSOs in Africa have an average staff strength of 15 individuals per organisation, with the smallest in our focus group having 6 staff members and the largest having 31 staff members. While it only takes one human error for an organisation to become a victim of a social engineering attack, having a smaller workforce may mean that CSOs in Africa are potentially better positioned to manage the human element in protecting their digital safety since they have only a few people to manage.

A larger workforce, on the other hand, may indicate a higher number of potential touch points and may require a more robust security infrastructure with more investment in human resources management to mitigate the risks associated with a wide staff base.

Among these members of staff, CSOs within our focus group state that there are none whose social profile poses a direct risk to the organisation. However, top-level personnel, particularly board

“

While frontline staff pose minimal risk to CSOs, board members emerge as potential triggers for cyber attacks.

Securing high-profile personnel becomes imperative, highlighting the need for tailored security measures beyond the general workforce.

”

members of many of the CSOs, were identified as potential triggers for cyber attacks from bad actors. In essence, security measures for CSOs in Africa ought to extend beyond the general workforce to specifically address the vulnerabilities associated with high-profile personnel who may be targets of malicious actors.

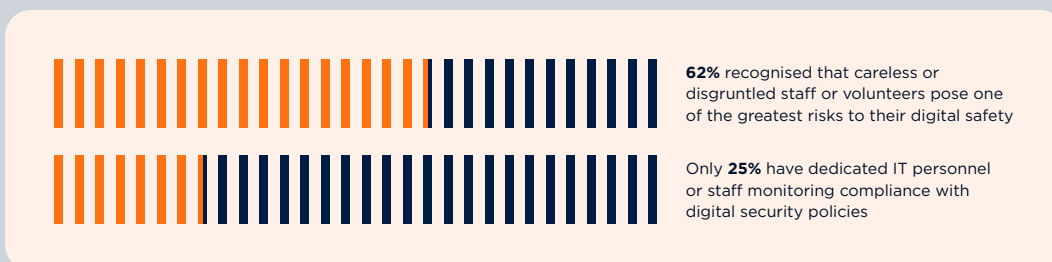
The shift towards remote work due to COVID-19 has introduced a new dimension to digital security for CSOs, as most CSOs in Africa now have a virtual component to their work, either being fully remote or hybrid. This obviously impacts their level of exposure and necessitates enhanced cybersecurity measures requiring remote access policies, prioritising secure communication channels, and ensuring continuous monitoring to mitigate the increased vulnerability associated with virtual operations.



Another human factor detected from our assessment is the volunteer-heavy nature of 62% of CSOs within our focus group. This introduces a unique set of challenges for digital security, as volunteers are often external to the organisation and may not be subject to the same level of scrutiny as regular staff, posing potential risks. Therefore, organisations need tailored strategies, clear guidelines, and monitoring mechanisms for managing their volunteers.



Our assessment also revealed that only 25% of CSOs have staff that have received any previous digital security training, and none (0%) of the CSOs require their staff to ever undergo any digital security training. The low percentage of staff receiving digital security training, coupled with the absence of mandatory training requirements, signals a critical gap in preparedness, a significant component of digital resilience. Digital security education must therefore be prioritised by CSOs and at-risk communities to empower their staff and volunteers with the skills needed to recognise and respond to potential threats.



Finally, while about 62% of the focus group recognised that careless or disgruntled staff or volunteers pose one of the greatest risks to their digital safety, only 25% have dedicated IT personnel or staff in charge of managing other staff and monitoring compliance with digital security policies. In fact, in most cases, no one at all is responsible for digital security in their organisation.

B. Process

As part of our assessment, we reviewed processes within the organisations that related to their digital security. For instance, processes for managing and accessing shared accounts, social media accounts, managing web domain(s), revoking staff access, and so on. The data obtained from this aspect of the assessment is important because the processes—or lack thereof—within an organisation reveal whether digital security is standardised and consistent and whether compliance and governance are subject to an unbiased set of protocols that would ensure the sustainability of digital security policies.



Our assessment revealed that 75% of the organisations do not have a uniform process for accessing shared accounts beyond every staff member having the password to the account. This raises concerns about traceability in the event of a breach of the shared account. However, half of the focus group displayed more proactivity in creating hierarchical access controls, limiting certain staff members from accessing specific classes of data.

Only 50% of the organisations established processes for periodic reviews of data access, raising concerns about potential dormant accounts with privileges. The lack of regular access reviews reveals a security gap, as it becomes challenging to promptly identify and address unauthorised access, leaving organisations susceptible to insider threats.


Perhaps more damning is our finding that only 37% of the organisations have a process for revoking access after a staff member's exit or

termination from the organisation. Recall that most of these organisations indicated that they consider disgruntled staff or ex-staff as some of the biggest risks to their digital security. Even moreso, some of the organisations' approach to revocation of access involves waiting periods after termination, which may seriously impact data integrity.

Furthermore, only half of the organisations within the focus group have dedicated IT personnel managing their web domains. The other half simply has the domain credentials, which may then be shared with any staff or external person as the need arises. Interestingly, the

organisations with dedicated IT personnel, however, largely revealed that they lacked or were unaware of specific web security processes in place.

The assessment also revealed two prevalent methods employed by CSOs for protecting access to social media accounts: password and multi-factor authentication, or restricting access to a limited number of individuals. Both approaches have their pros and cons. Passwords and multi-factor authentication enhance security but may pose challenges in cases of high staff turnover unless effective password management is observed and reconfiguration of MFA settings is done as needed.



**“
Access management
emerges as a critical concern,
with 75% of organisations lacking
uniform processes for shared
account access, raising traceability
issues in the event of breaches.
”**

Conversely, limiting access reduces the risk but may impede operational efficiency.

A mere 12% of the CSOs had a documented contingency plan for incidents like accidents, device loss, or staff incapacitation during transit. The implications of this gap are far-reaching, including potential data loss, compromised security, and operational disruptions.

Additionally, no single organisation within the focus group had a process for following up with staff after a security incident. The complete absence



of follow-up processes raises concerns about organisational learning and the potential of enhancing security measures over time. Finally, none of the organisations had documented security protocols.

This lack of formalised guidelines leaves CSOs and at-risk communities vulnerable to inconsistent practices, which in turn hinders effective communication about security measures and compromises their overall preparedness to face threats to their digital safety.

C. Technology

Perhaps more popular is the role of technology in the digital security of any organisation. Under this category, we sought to assess each organisation's culture with software, hardware, and communications technologies in order to determine their security posture.

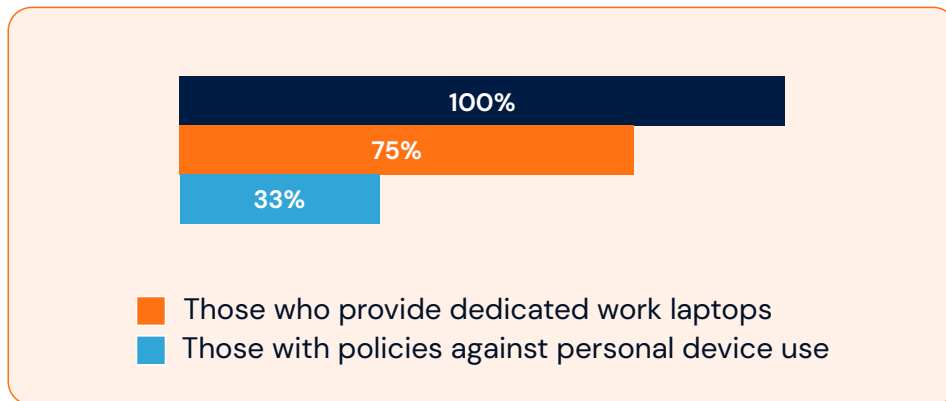
A substantial 75% of organisations within our focus group utilise a combination of cloud storage and external hard drives for their data storage, while 24% exclusively rely on local storage methods such as computers, hard drives, or paper. The prevalence of cloud storage reflects a recognition of its convenience and accessibility.

For organisations that use cloud storage, access to data is granted via sharing features on that cloud storage software. For organisations that do not use cloud storage, they do not have a clear way to share their data. While some use instant messaging platforms or email, others simply could not articulate how they share their data.

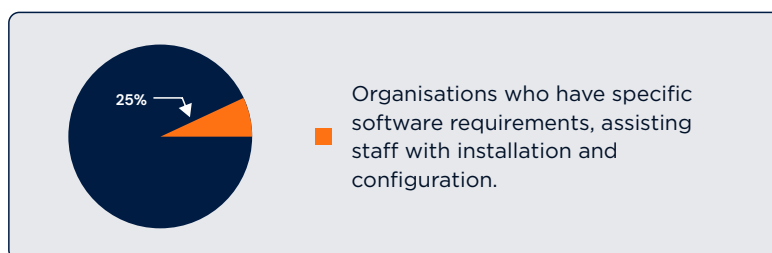
The lack of a standardised data-sharing method poses risks, and relying on ad-hoc methods like WhatsApp or email may compromise data security and organisation-wide access.



Similarly, 75% of organisations provide dedicated work laptops, but only 33% enforce policies disallowing staff from using personal devices. While dedicated work laptops enhance security, the laxity in restricting personal device usage may introduce potential vulnerabilities. Organisations should consider reinforcing policies to mitigate the risks associated with personal devices, such as unsecured connections and unauthorised access.



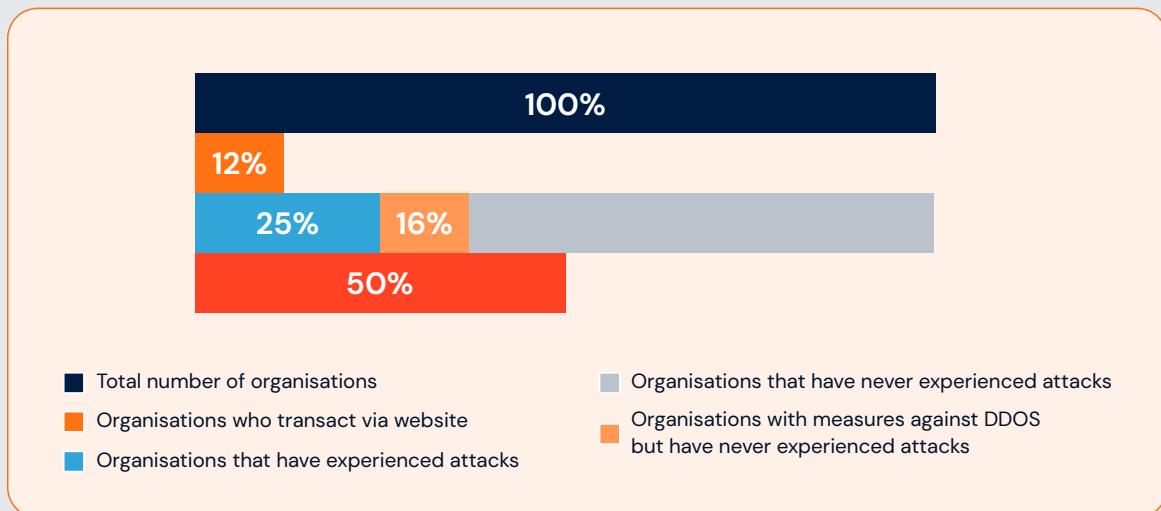
Regarding software configuration and installation, 25% of the organisations within our focus group have specific software requirements, assisting staff with installation or configuration. Others use pre-installed or pre-configured software. It is important to note that the manner in which software is managed affects both security and functionality, and organisations with dedicated software requirements demonstrate proactiveness in ensuring staff have the necessary tools. Conversely, reliance on pre-installed software may limit customisation and security control.



Still, regarding software, 50% of the organisations use or have used paid versions of essential software, while the rest rely on free alternatives or none at all. Opting for paid software often provides additional security features and regular updates. Hence, organisations that use free versions or none at all are potentially exposed to increased security risks.

From our assessment, we found that CSOs primarily communicate via popular tools like Google, Zoom, Signal, Whatsapp, Asana, Flock, Facebook, and direct calls. The most popularly used product for emails is Google. When asked about using encrypted communications tools, most of them indicated that they use WhatsApp, and only 12% indicated the use of Signal or Flock. While widely used platforms are more available and are not necessarily a bad option, the limited adoption of encrypted tools raises concerns about the privacy culture and awareness within these organisations, as having an option for more secure communications is crucial for protecting against digital threats.

Finally, only 12% of the organisations within our focus group use their website for financial transactions. 25% have experienced actual attacks on their websites; however, only 50% of those organisations have a measure in place to prevent Distributed Denial of Service (DDoS) or Denial of Service (DoS) attacks. Out of the remaining 75% of organisations that have not experienced any attacks on their websites, only 16% have put in measures to prevent DDoS attacks.



D. Policy

Only 12% of the organisations within our focus group had a digital security policy. This has a myriad of obvious implications, such as inconsistent security practices, which were indeed observed, a lack of employee awareness and training, poor incident response and recovery, and preventable breaches and losses.

When asked what data they considered important, the organisations listed financial data, beneficiary data, stakeholder data, proposal information, field data, research data, public data, and employee data. When asked to rank, the data ranked as most sensitive were financial data and beneficiaries' personal information, while the data ranked as least sensitive were public data and employee data.

However, as stated, the majority of organisations had no security policy in place to secure these data. From our observation, the absence of these policies has resulted in ad-hoc security measures, leaving the organisations vulnerable to overlooked threats, inconsistent security practices, and a lack of clear guidelines on how to respond to security incidents. This organisational posture has also impacted employee knowledge and the overall security culture, as a lack of clarity in roles can result in a fragmented approach to security with no clear ownership over initiatives.



5.0 Identified Risks and Vulnerabilities

When asked what risks they are most concerned about, organisations listed, physical harm, virus, loss of data, phishing, hacking, doxing and ransomware. Here are however, some of the risks and technical vulnerabilities identified from an aggregate of assessments; DOM data manipulation, unencrypted connections, weak or missing security headers like X-Frame-Options or Content-Security-Policy, poor and vulnerable authentication, vulnerable JavaScript libraries, Strict transport layer security (TLS) not enforced and cross-site scripting.



6.0 The Resilience Design Intervention

In response to the findings from the comprehensive assessments conducted on the organisations within our focus group, we recognise the imperative to not only identify vulnerabilities but to proactively contribute to their digital resilience. As part of our intervention strategy, we crafted a tailored approach—The Resilience Design—to empower these organisations with the tools and knowledge necessary to fortify their digital security.

In light of this, each organisation received these interventions:

A. The Digital Wellness Check Report

Using the Digital Wellness Check (developed by the [Center for Digital Resilience](#)), we provided the organisations with a diagnostic report containing insights into their current digital health, strengths, and areas that warrant attention. The report contains an appreciation of the context within which the organisation works. Risk is then assessed based on the following categories: data, devices, communication, physical security, education, external services, contingency plans, responsibility, policies, and privacy. Each category is explained with tailored recommendations and actionable steps for targeted improvements from our team of experts.

B. Website/Infrastructure Assessment

After conducting an independent and comprehensive assessment of each organisation’s website security, we created a report evaluating the health of the website; identifying vulnerabilities and equally providing recommendations for tighter security. In the report, we identified vulnerabilities and rated them according to levels of severity. These specific insights were helpful for organisations to take action for their digital resilience.



C. Comprehensive Digital Security Policy

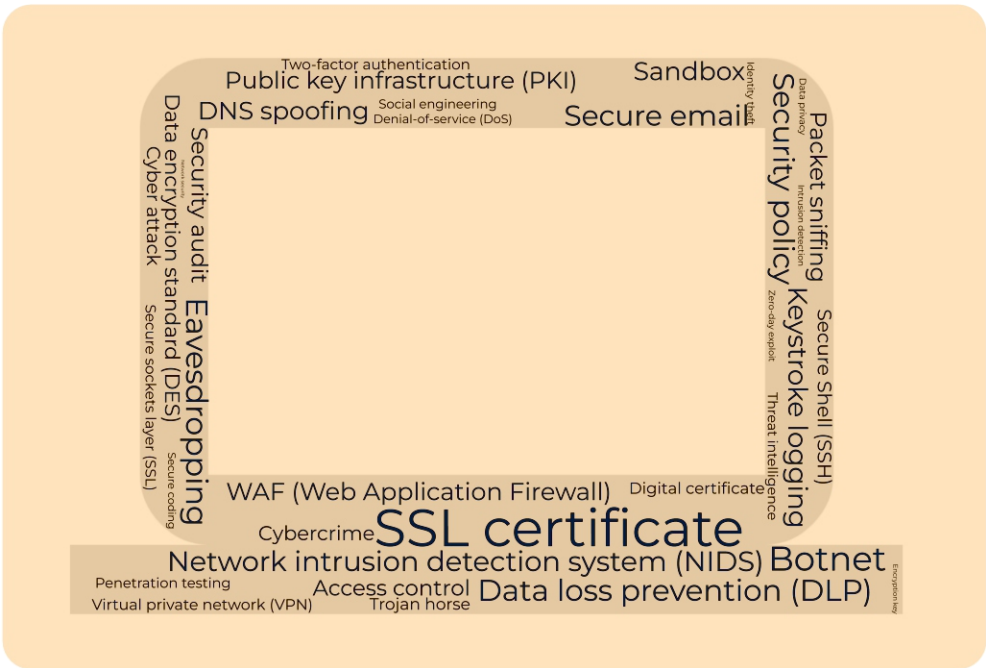
We developed a robust digital security policy based on their unique needs. Depending on specific organisational requirements, the policy contained provisions on devices, communication, accounts, travel, environment, and network. The document also contains clear guidelines and checklists to help operationalize the policies.

D. Organisational Training

Apart from the documents shared, we also conducted an organisation-wide training for each organisation. The objectives of the training were to equip staff with practical skills and techniques to mitigate common security risks in day-to-day operations and to foster an organisation-wide understanding of the newly crafted digital security policy and its relevance to their daily activities.

E. Post-Training Assessment

Following the initial training period, a critical component of our Resilience Model was the post-training assessment conducted 6-8 weeks afterwards. This assessment was carried out for the individual employees/volunteers who underwent the organisational Training. Via this assessment, we aimed to evaluate the assimilation of cybersecurity knowledge and practices among the trained staff. Below are our findings.



7.0 Findings

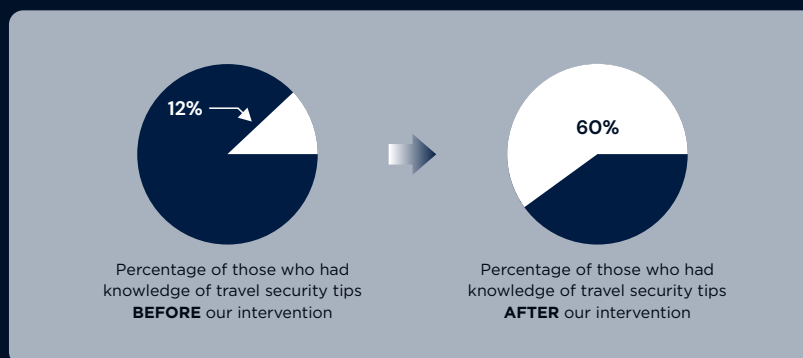
Trainees were tested on passwords, security policies, social media, travel security, data classification, encryption, data classification, data retention and disposal, and malware.

100% of respondents displayed increased knowledge of creating and using strong, memorable, and secure passwords. They indicated that they had learned to now use a password manager for unique passwords and to also regularly update passwords with a mix of characters.

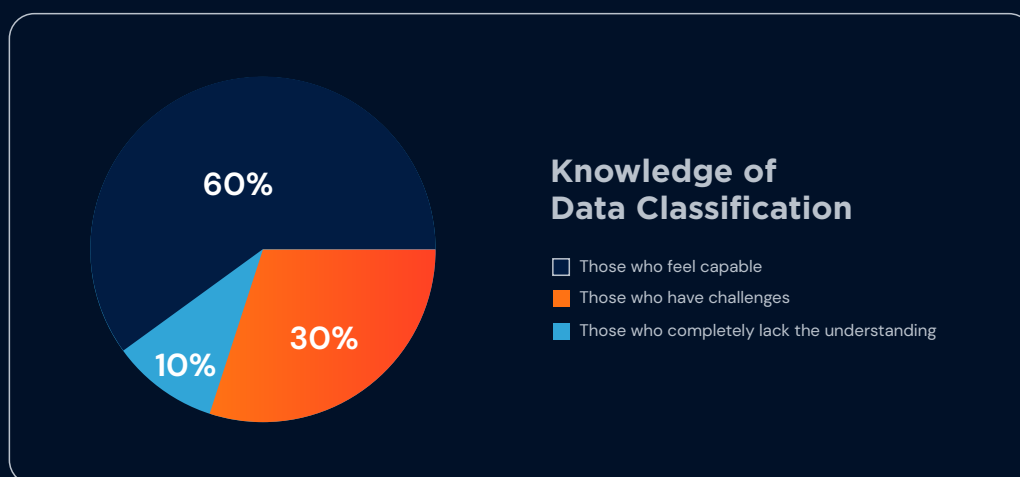
Recall that none of the organisations had digital security policies and that a part of our intervention was to tailor-make digital security policies for each organisation. The assessment revealed that trainees knew to now follow organisational security policies consistently and, for those who lead teams, to communicate the policies regularly, leading by example and conducting regular training.



60% of the respondents displayed an increase in knowledge of travel security tips, knowing to not share sensitive knowledge on public networks, to use VPN for a secure connection, to avoid public WIFI for sensitive tasks, to ensure devices are password protected, and to limit social media and prioritise safe travel, whereas only 12% had displayed such knowledge prior to our intervention.



While 100% of respondents displayed an increase in knowledge of data classification, retention, and disposal, 60% felt capable enough to navigate the complex landscape of data protection compliance. 30% indicated that they have challenges navigating compliance requirements, while 10% indicated that a lack of understanding regarding compliance processes is a problem.



Finally, when asked which of the digital security practices they had successfully incorporated into their day-to-day activities, they mentioned: the use of strong passwords, stricter use of the principle of least privilege, exhibiting more caution for phishing scams, updating passwords regularly, using two-factor authentication, implementing a data backup strategy (the 3-2-1 strategy), prioritising secure communication, especially for sensitive data, and administering or relaying the training they received to other members of the team.

8.0 Challenges: Why a Project Tagged 'RT-10' Had Only 8 Participants

At the conceptualization and announcement of the RT-10 project, we had undertaken to engage 10 organisations within the focus group, hence the tag 'RT-10'. However, as some of the percentages above reveal, we ended up working with 8 organisations even after an extension of the timeline and a second call for applications. As we reflect on the overall project, we believe that this experience may have an inherent value in terms of lessons and insights for the CSO community and its stakeholders. As part of our organisational learning efforts, the team has debriefed, and we, herein, present our perspective on the perception of cybersecurity by CSOs in Africa as well as some other project management feedback for the community.

It must be stated that while the challenges we encountered impacted the scope and reach of the initiative, they did not impact the quality of the assessment and findings discussed.

A. Cybersecurity Non-Prioritisation

We observed a prevailing attitude of nonchalance by many CSOs towards cybersecurity. Most CSOs are aware that cybersecurity is important, but not many convert this into real prioritisation for the organisation. On this project, we found that securing commitment was difficult for many organisations that had indicated interest even though our services were going to be free.

B. Staff Constraints

We also observed that the size of the organisations' workforce also contributed to how effectively they could participate in the assessments. Many CSOs in Africa are grappling with staffing constraints and this inhibits their ability to allocate personnel to external initiatives like the RT-10 project whilst simultaneously requiring those personnel to work on their routine organisational tasks.

C. Poor Email Communication Culture

Instances of infrequent email checking and delayed responses were pervasive, leading to a communication gap, which in turn contributed to delays within our implementation timeline. In the future, we will incorporate an alternative means of engagement, such as utilising more familiar platforms like WhatsApp, to ensure effective and timely communication.

Effects of the Challenges

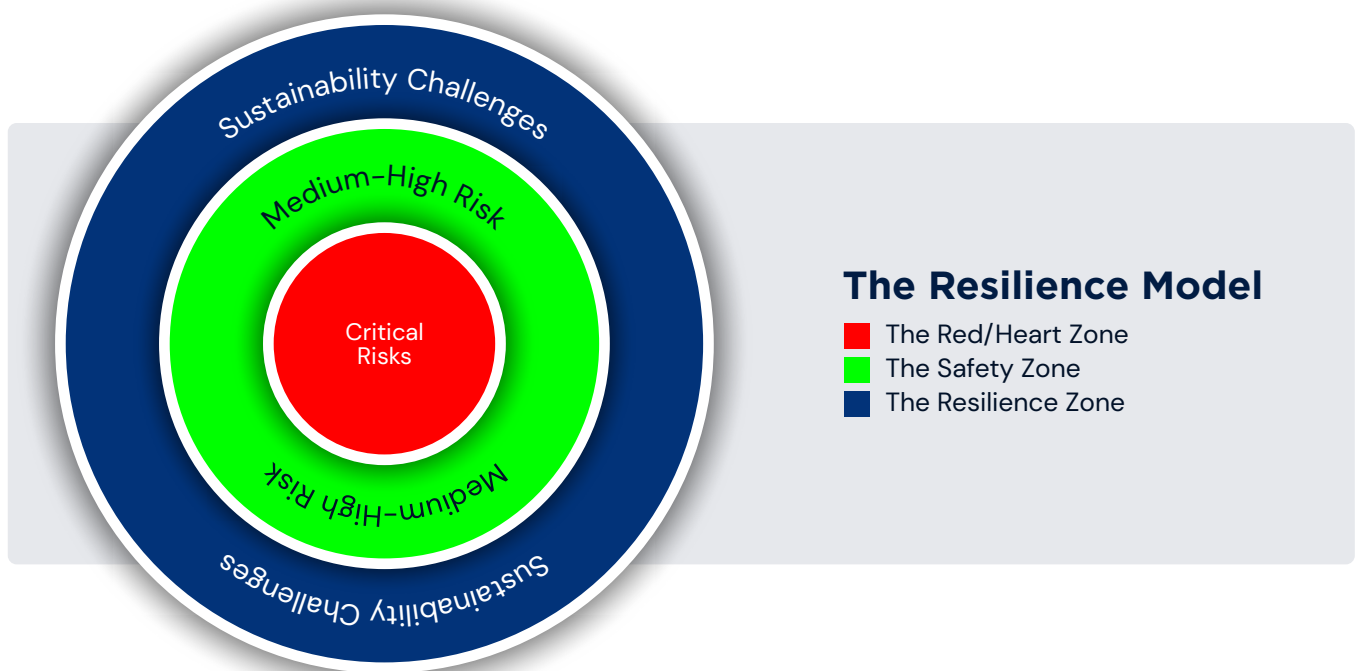
These challenges significantly impacted the scope and timeline of our project. However, it is not out of place that such challenges may have farther-reaching effects on the motivation of cybersecurity consultants, funders, and other stakeholders to invest in much-needed cybersecurity intervention initiatives.



9.0 The Resilience Model: Our Recommendation

What is the Resilience Model?

The Resilience Model is a guiding framework and approach to holistic digital security assessment and intervention for civil society organisations. The Model explores the various digital risks civil society organisations are likely to face or be exposed to, and categorises these into three layers, by severity of impact of the risks in that layer.



As seen in the image above, the Resilience Model shows three core layers that collectively define the resilience of an organisation to digital threats and attacks. It holds that for an organisation to truly be resilient, it must have three strong layers: a sturdy core, a safe middle zone, and a truly resilient outer shield.

The Red or Heart Zone:

As it implies, this zone represents the region closest to the heart of an organisation; hence, risks (or interventions) here can critically impact an organisation and affect its continuous ability to remain operational (at least for an extended period so that it results in significant business and operational losses).

Examples of threats and risks in this region include data breaches and data exfiltration, business email compromises, key account compromises, ransomware attacks, insider threats, spyware attacks, regulatory compliance issues, and so on.

Digital security interventions here are the most common, as organisations and security providers both understand how damning the risks in this region can be and the need to ensure that they are properly mitigated and addressed.

Impact of Risk: Critical

Safety Zone: This zone or layer captures the risks and threats that can either affect the public image or perception of an organisation or the functionality of some of its operations (or both). The impact of risks here is usually between medium and high, but they do not have the capacity to cripple an organisation's operations or result in any significant business losses; hence, they are called a safety zone, implying that organisations that take care of this zone can be termed safe.

Some of the risks here include DDOS/website attacks, poor backup regimes and practices, social media account issues, network downtime, and minor regulatory issues.

Impact of Risk: Medium to High

The Resilience Zone: This is the zone where true resilience exists. It is the outermost and most protective layer in the resilience model. Without this, an organisation quickly falls back to the practices that once made them susceptible to digital attacks. Because of the time it takes to implement this layer (and the corresponding time to see the impact of it), this layer is often ignored in security interventions for civil society organisations. Hence, we truly do not see proper resilience interventions, only digital safety, which is not sustainable. The Resilience zone captures interventions that support an organisation's continuous ability to remain resilient against digital attacks without external influence or help.

This layer is marked by behavioural change and situational awareness of digital security incidents, backed and enabled by policies, consistent training, and assessments. Its goal is to make sure that an organisation can effectively stave off and mitigate internal and external threats to its operations and assets with minimal external support or intervention.

The Resilience Model is further defined by 5 key factors or characteristics:

A. Holistic

An organisation cannot boast of true digital resilience until it is complete in its approach to tackling digital risks and concerns within the organisation. That means that careful assessment and implementation plans must be followed for all three zones or layers, as described above.

B. Rapidness

Digital security interventions must both be holistic and swift to avoid leaving gaps and loopholes for threat actors, especially in an industry like the Internet Freedom space where attacks are carefully planned and are often successful thanks to the scarcity of cybersecurity talents supporting organisations (especially in the global south).

C. Long-term

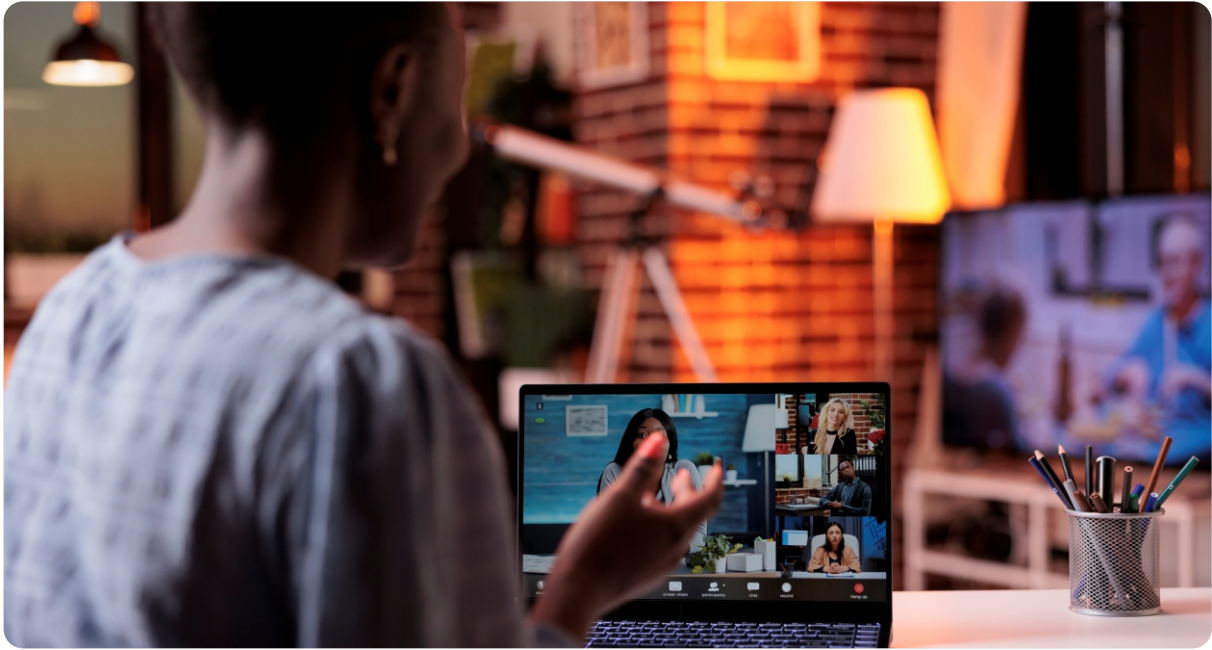
Approaches to digital security interventions must have a long-term outlook. This is the case for any true intervention, but it is especially so with civil society organisations, as many organisations cannot afford to have recurrent or periodic assessments and audits. Hence, any intervention in civil society must be for the long term.

D. Cost-effectiveness

The average civil society organisation does not have money to fund its core operations, and that means even less money to pay for digital security services. For organisations to embrace a suite of resilience measures, the Resilience Model posits that those measures must exist within a certain price focus; otherwise, they instantly become inaccessible to the average organisation.

E. Sustainability

The sustainability factor describes the extent to which an organisation can detect, contain, mitigate, and respond to digital threats and attacks without any external help or intervention. This is the one main factor that defines true digital resilience for any organisation and includes all interventions in the Resilience layer of the Resilience Model.



10.0 Conclusion

The comprehensive assessments conducted on our focus group of Civil Society organisations (CSOs) in Sub-Saharan Africa have revealed both strengths and vulnerabilities. We found that African CSOs operate with a marked shift towards remote or hybrid work models, driven largely by the challenges posed by the COVID-19 pandemic.

While staff numbers are relatively modest, a concerning divide still exists in digital security awareness, and board members and top-level personnel emerge as potential risk factors, necessitating targeted security measures to mitigate potential attacks.

We also found that a significant gap in digital security training is evident, with only 25% having staff trained and none mandating ongoing training for their personnel, despite most organisations being volunteer-heavy. Inconsistent processes for accessing shared accounts and varied approaches to data access control are prevalent, exposing organisations to potential breaches, and only a quarter of organisations with website attacks have measures to prevent DDoS or DoS attacks, highlighting vulnerabilities in website security.

Finally, we found that most of the CSOs in our study do not have a standardised organisational digital security policy. We have set forth the Resilience Model, in the body of this report as our recommendation to the security community in their interventions for Civil Society Organisations and at-risk communities.

There are, however, still opportunities for further research, and we encourage researchers and enthusiasts to explore other areas not covered in our research, such as the complexity of data protection compliance processes across the continent, the impact of remote or hybrid work on the digital security of CSOs in Africa, the long-term effects of digital security training on the output of CSOs, and a comparative analysis of digital security realities for CSOs in Africa and other regions.

Published by:



RESILIENCE
TECHNOLOGIES

www.rtafrica.org