WACSI
WEST AFRICA CIVIL SOCIETY INSTITUTE

CHARLES STEWART MOTT FOUNDATION®

RESEARCH REPORT

LANDSCAPE MAPPING OF CIVIL SOCIETY DIGITAL SECURITY IN WEST AFRICA

MARCH 2023

Research Team

Lead Researcher
Evans Tindana Awuni

Research Assistants
Belinda Bakah
Emmanuel Foli Mawusi
Eric Agidi Dunyo
Mohammed Mudasir Yussif
Moshie-Dayan Laminu
Mubarik Abdul Mumin
Ronald Kouago
Theophile Kwame Atonon

Editorial Team

Jimm Chick Fomunjong
Franck Sombo
Nancy Kankam Kusi
Stella Yawa Wowoui
Mabel Shu
Whitnay Segnonna

Disclaimer: The authors remain responsible for any errors and omissions in this report.

For more information, write to:
West Africa Civil Society Institute
(WACSI)
P.O. Box AT1956 Achimota
Accra, Ghana
Email: info@wacsi.org
Tel: (+233) 303937264

Cite as: **WACSI (2023). Landscape Mapping of Civil Society Digital Security in West Africa, Accra, Ghana.**

ACKNOWLEDGEMENTS

Globally, technology is evolving at a fast pace. It is increasingly becoming an indispensable asset for existence and more so, for the effective functioning of institutions. Despite this, civil society organisations (CSOs) in West Africa lag in terms of fully maximising the full potential and breadth of opportunities provided by technology. This lag can partly be attributed to the risks technology exposes its users to.

Unfortunately, in West Africa, in recent years, bits of information have been shared on the menace posed by digitisation to actors within the civil society ecosystem. However, the extent to which the work of civil society actors is aided or hampered by digitisation has not been comprehensively examined.

The West Africa Civil Society Institute (WACSI), in the wake of its 2023 to 2027 strategy, which has a focus on ensuring that CSOs are adequately supported to leverage technology to promote their developmental initiatives, commissioned this study to have a holistic appraisal of how digital security affects the work of CSOs in the region. While this is critical in informing and shaping the Institute's work going forward, it constitutes a rich body of knowledge that can inspire a diverse pool of stakeholders to contribute, together with WACSI, to improve the digital landscape to enable the work of CSOs.

WACSI commends the Mott Foundation for the support that enabled this research to be carried out. Thanks also go to the team that facilitated the execution of this research work; Franck Sombo, Kwame Asante, Stella Wowoui, Whitnay Segnonna, Nancy Kankam Kusi, Shu Mabel Lum and Jimm Chick Fomunjong for assiduously ensuring that this body of work is executed.

WACSI extends its sincere gratitude to all the survey respondents from the civil society organisations (CSOs) in West Africa that formed part of this study. We appreciate your willingness to share your experiences and insights on the digital security challenges facing CSOs in the region. Your contributions have been invaluable in helping us better understand the digital security landscape for CSOs in West Africa and in shaping the recommendations presented in this report. It is our hope that these valuable insights will enable us, our partners and other stakeholders to design relevant tailor-made programmes to improve the digital landscape in your particular interests.

We also acknowledge the key informants who provided us with additional insights and perspectives on the digital security issues facing CSOs in the region. Your contributions have been instrumental in expanding our understanding of the challenges and opportunities in the digital security space for CSOs in West Africa.

Special thanks also go to our research team members who worked tirelessly to ensure the success of this study under the able leadership of Evans Tindana Awuni.

Finally, we would like to express our appreciation to the wider community of digital security researchers and practitioners who have contributed to the development of this field. Your insights and innovations have been an inspiration and have helped us in implementing this study.

Nana Asantewa Afadzinu
Executive Director

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF BOXES (CASE STUDIES)

LIST OF ACRONYMNS

ANLC: National Authority for the Fight Against Cybercrime

ANSI: National Agency for Computer Security

ANTIC: National Agency for Information and Communication Technologies

AU: African Union

CBO: Community Based Organisation

CFA: Communauté Financière Africaine Franc

CIVICUS: World Alliance for Citizen Participation

COVID: Coronavirus Disease

CSO: Civil Society Organisation

DDoS: Distributed Denial of Service

DPA: Data Protection Agency

ECOWAS: Economic Community of West African States

GDPR: General Data Protection Regulation

GMD: Gambian Dalasi

HAPDP: High Authority for the Protection of Personal Data

ICMEC: International Centre for Missing and Exploited Children

ICT: Information and Communication Technology

IDPS: Intrusion Detection and Prevention Systems

INGO: International Non-Governmental Organisation

INTERPOL: International Criminal Police Organisation

KII: Key Informant Interview

LCCPMA: Liberia Cyber Crime Prevention and Mitigation Agency

MDM: Mobile Device Management

NITDA: National Information Technology Development Agency

NGO: Non-Governmental Organisation

RAT: Remote Access Trojan

SNC: Senegal's National Cybersecurity strategy

UNCTAD: United Nations Conference on Trade and Development

UNESCO: United Nations Educational, Scientific and Cultural Organisation

USD: United States Dollar

VPN: Virtual Private Network

WACSI: West Africa Civil Society Institute

WIFI: Wireless Fidelity

Executive summary

In today's digital age, organisations are constantly exposed to various digital security threats. For civil society organisations (CSOs) in West Africa, the threat of cyber-attacks and data breaches is a real and growing concern. This study aims to shed light on the digital security challenges facing CSOs in West Africa, and to provide recommendations on how they can better protect themselves against digital security threats. By examining the most common threats, the exposure of CSOs to these threats, their preparedness to respond, and the effectiveness of national and organisational level policies, the study provides an in-depth analysis of the digital security landscape in West Africa.

Chapter one of the report introduces the study. It outlines the background and the rationale for the study, which is to investigate the digital security situation among CSOs in West Africa. The chapter states the key objectives of the study, including identifying the most common digital security threats facing CSOs, examining their exposure to these threats and their preparedness in responding to them, and exploring the policies in place at both the national and organisational levels to address these issues. The chapter concludes with a summary of key findings and an overview of the report structure to guide readers. Overall, Chapter one sets the stage for the rest of the report.

Chapter two takes a closer look at the most common digital security threats facing CSOs in West Africa. The results show that almost one-third (1/3) of the sampled CSOs have fallen victim to digital security attacks in the last twelve months. The most common types of attacks were computer virus attacks that harmed data (48%), followed by threats through social media (43%) and email (33%). When it comes to the geographical distribution of these attacks, Nigeria leads with 10.75% and Ghana follows close behind with 5.38%. The frequency of these attacks is also concerning, with at least 25% of the digital security attacks occurring multiple times in a year. These attacks take various forms, including those caused by humans, such as malicious insider attacks, personnel loss, human error, espionage, data integrity loss, phishing campaigns, theft, malicious code, and deceptive domain attacks, as well as technical ones such as software and malware failure, and those caused by nature, such as fire outbreaks, rainfall and extreme weather conditions. Furthermore, the results indicate that different types of CSOs experience different types of attacks. Community-based organisations (CBOs) and local NGOs (LNGOs) experience the highest rates of attacks compared to international NGOs. However, no statistical relationship was observed between the level of digital security and how established (or how old) a CSO is. Key informant interviews add further insights to the types of digital security threats faced by the CSOs in West Africa. The informants reported various hacking attacks on the CSOs' websites, social media accounts, and unauthorised access to the organisation accounts by a former employee. Human error that resulted in a computer being infested with viruses, data loss, phishing, malware attacks, and theft of ICT tools were also reported.

Chapter three highlights the adoption of digital technologies by CSOs and the practices they have in place to secure their digital assets. With 99% of CSOs relying on email, 97% using laptops or desktop computers, and 89% using mobile phones or tablets, digital technologies play a crucial role in their operations. However, with only 44% of respondents being aware of their organisation's digital protection, and 70% having no digital security training, CSOs in West Africa are facing significant exposure to digital security threats. The report reveals that while 95% of CSOs use strong passwords, they tend to neglect other secure digital practices. Only 51% of respondents reported updating their operating system with the latest security patches, and a mere 20% relied on virtual private networks (VPNs). The situation is compounded by the fact that 70% of CSOs report a lack of financial capacity to allocate a budget for information security. This chapter sheds light on the need for CSOs to prioritise their digital security and invest in necessary measures to protect themselves from potential digital threats and attacks.

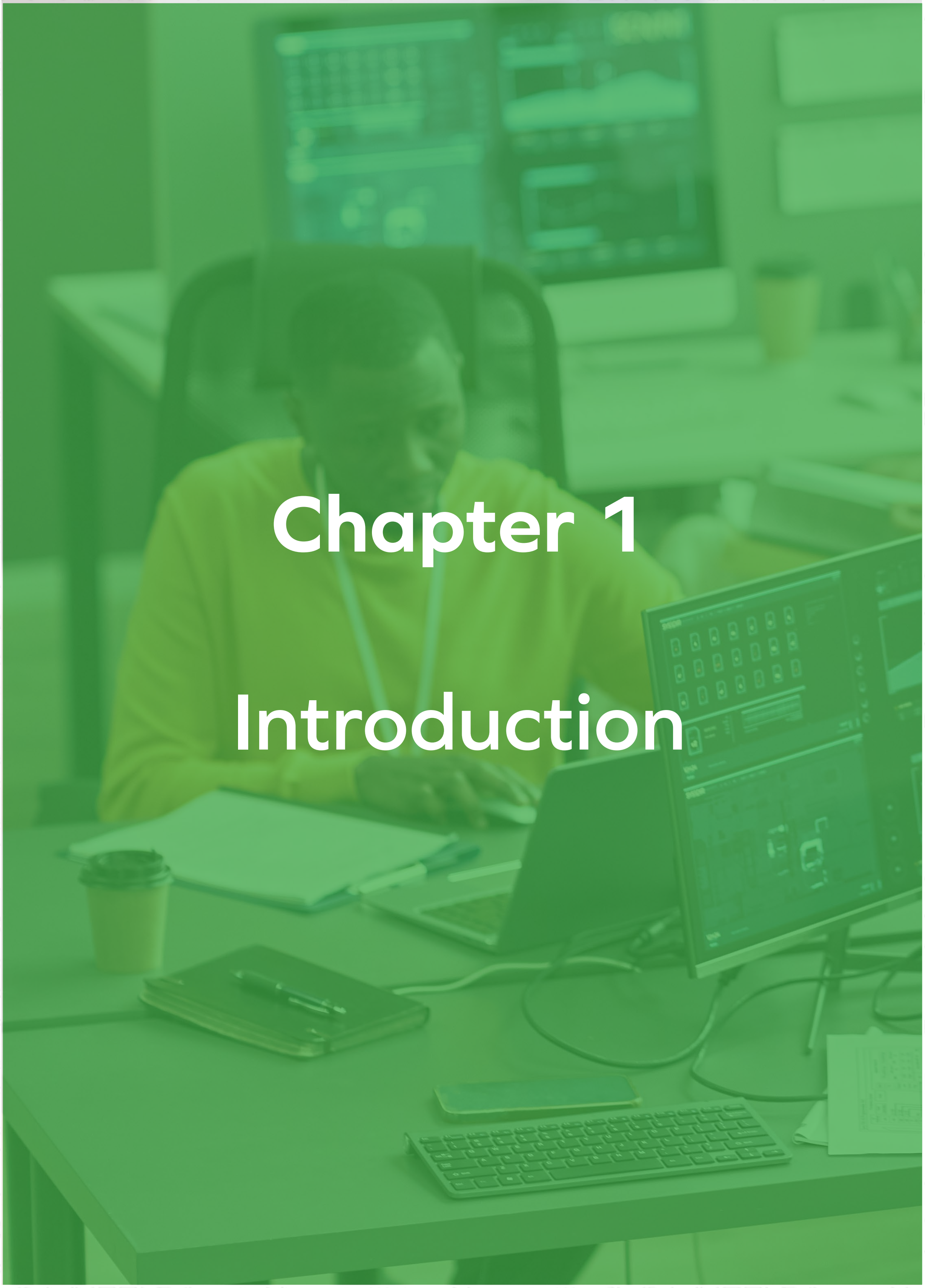
Despite the widespread adoption of ICTs among CSOs in West Africa, the findings in chapter four of the report highlight a concerning lack of preparedness when it comes to securing their digital operations and responding to digital security threats. With only 30% of CSOs reporting participation in digital security training programs, much more needs to be done to educate and empower these organisations to effectively defend themselves against cyber attacks. The chapter delves into the topic of digital security interests among West African CSOs and highlights key words such as "data," "security," "system," "device," and "protection" as the most cited by the respondents. This further underscores the eagerness of CSOs in acquiring knowledge about protecting data, digital devices and system against attacks, and the need to prioritise it in training and capacity building efforts. The chapter concludes with a series of recommendations aimed at facilitating the creation of effective digital security training programmes for CSOs in West Africa. The results of this study emphasise the importance of investing in digital security education and providing CSOs with the tools and knowledge they need to operate securely in the digital space.

In chapter five, the focus is on the national level digital security laws and policies in West Africa. The key insights show that while nearly all West African countries have policies in place to protect personal data, 45% of CSOs are not aware of these policies. Half of the countries have dynamic policies that are often updated. While almost all countries have some form of a data protection regulation in place, only six (6) countries in West Africa (Benin, Burkina Faso, Cape Verde, Ghana, Mali and Senegal) have comprehensive data protection laws. Also, only Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Ghana, Nigeria, Sierra Leone, and Togo have developed relatively comprehensive national policies and laws to fight digital crime. Yet, in most cases, enforcement of these laws is either weak or non-existent, and capacity building on digital security remains a challenge for many West African countries. This chapter highlights the need for increased awareness and implementation of digital security laws and policies in West Africa to promote the safety of individuals and organisations.

Chapter six delves into the organisational level digital security policies or strategies, revealing not only nonexistence of ICT policies in CSOs but also a lack of proper implementation and understanding among CSOs in West Africa. Only 23.6% of the surveyed CSOs have a computer and information security policy in place, with 24% reporting not understanding the contents of the policy and 27% deviating from it at times. The trend of working from home and other locations with vulnerabilities such as not using VPN connections, the use of personal digital devices for work activities, among others, only exacerbates these security risks. These findings together with the numerous digital security breaches CSOs have suffered, highlight the urgent need for CSOs in West Africa to implement stronger and well-understood digital security policies to protect themselves from potential attacks.

In Chapter seven, the report sheds light on the major digital security challenges facing CSOs in West Africa. The findings indicate that finance remains a major challenge, with most CSOs dependent on donor agencies and philanthropists, and vulnerable to fraudsters posing as genuine funders and requesting sensitive information. The lack of ICT infrastructure limited digital security infrastructure, the absence of well-resourced IT units, and insufficient digital security training are further hindrances. Furthermore, the limited availability of organisational-level digital security policies, combined with multifaceted national level policies that struggle to keep up with the rapidly changing digital security environment, further exacerbates the challenges faced by CSOs in West Africa.

The final chapter concludes and presents fifteen actionable recommendations aimed at improving digital security among CSOs in West Africa. These recommendations focus on improving the availability and accessibility of ICT infrastructure, increasing investment in digital security training and capacity building, establishing dedicated IT units within CSOs, and implementing organisational level digital security policies. The chapter concludes by emphasising the importance of addressing digital security challenges facing CSOs in West Africa and the need for a collective effort from all stakeholders in the region to ensure that CSOs are equipped to effectively respond to digital security threats and attacks. The study provides valuable insights and recommendations that can be used by CSOs, governments, policy makers, and development partners to improve digital security in West Africa.



Chapter 1

Introduction

The role of civil society organisations (CSOs) in promoting public discourse, accountability and community development is crucial in a functioning society. Aside from the government and the private sector, CSOs have emerged as the third force in the governance of a country (Florini, 2012; Scholte, 2002). They embody non-governmental organisations (NGOs), advocacy groups, informal social groups, faith-based organisations and other professional bodies such as the academia and media (Cooper, 2018). They peacefully and significantly mobilise communities for development (Jagalur et al., 2018). Overall, the role of CSOs is embedded in their activities, which seek to create a platform to sufficiently promote, discuss and address the felt needs of societies in ways that the government and private sector have often failed to do (Anheier, Lang, and Toepler, 2019; Lynn et al., 2022). They promote openness in public discourse and accountability of public officials in government transactions that seek to promote the welfare of the people (Jagalur et al., 2018).

As the world becomes increasingly digital, CSOs in West Africa are turning to new forms of technology to enhance their operations and achieve their objectives more efficiently and effectively (Lynn et al., 2022). These organisations are using digital tools for a variety of purposes, such as communication and outreach, fundraising and donation, advocacy and campaigning, data collection and analysis, organising and collaboration, and service delivery (see Table 1). Regarding communication and outreach, for example, CSOs are increasingly using social media, messaging apps, and video conferencing to connect with a wider audience and engage with stakeholders in real-time. Another example is fundraising and donation, where digital payment systems, crowdfunding platforms, and digital wallets are making it easier for CSOs to receive funds from various sources.

Similarly, in terms of advocacy and campaigning, CSOs use social media, messaging apps, and mobile technologies to raise awareness and mobilise support for various campaigns. They are also leveraging digital technologies like mobile data collection tools, data visualisation, and machine learning to collect, analyse, and disseminate data to gain insights and make informed decisions. Collaboration in organisations is also enhanced by the use of online platforms, project management and collaboration tools, allowing CSOs to easily share resources, knowledge, and expertise. Furthermore, the use of mobile apps, chatbots, and online platforms for service delivery is enabling CSOs to reach more people and deliver services more efficiently and effectively. Arguably, the COVID-19 pandemic and its associated mobility restrictions which limited the face-to-face activities contributed immensely to the increasing adoption of ICTs by CSOs.

Table 1: CSOs' use of digital technologies

Digital technology	Activity	Example
Social media platforms such as Facebook, Instagram, WhatsApp and Twitter	Information sharing and promotion	Information sharing, event promotion, advertising
Online forums and discussion boards such as Reddit; Virtual meeting platforms such as Microsoft Teams, Zoom, WebEx and Skype	Community Building	Recognition and gratitude, acknowledgement of events, dialogue and engagement
Online donation platforms such as GiveDirectly, JustGiving, and GoFundMe	Fundraising	Donation appeals, product sales, crowdfunding
Job listing websites such as LinkedIn	Recruitment and Management	Employees, volunteers and member recruitment and management
Social media platforms and Online advocacy platforms such as NationBuilder and ActionNetwork	Advocacy	Lobbying and advocacy

Source: Adapted from Lynn et al. (2022: 100)

However, the shift towards online interactions and transactions has increased the potential for digital security threats to these organisations (Tabrizchi and Kuchaki Rafsanjani, 2020). The increasing use of ICTs has created safe havens for online crimes and the targeting of CSOs. The lack of specialised digital security training, and unsecured computer systems have made West African countries vulnerable to digital security attacks. These attacks have consequences on CSOs which do not only compromise their online presence but also lead to financial losses, psychological harm and reputational damage.

In 2016, the African Union (AU) adopted a policy on digital security to promote a safe and secure digital environment in Africa, recognising the increasing importance of digital technologies in driving economic growth, social development, and political participation, as well as the growing threats posed by cybercrime, cyber-espionage, and other malicious activities. While some African countries are developing legal frameworks to ensure digital security, enabling organisations, especially CSOs, to develop digital security programmes tailored to their needs, policy implementation has been problematic. A lack of technical capacities and national digital security programmes that accommodate CSOs in West Africa has been observed (Bada, Von Solms and Agrafiotis, 2019; Eboibi, 2020), emphasising the need for a comprehensive investigation into the preparedness of CSOs in West Africa to respond to digital security threats.

Considering the crucial role that CSOs play in promoting transparency in public discourse and ensuring accountability of government officials in their transactions, coupled with the growing exposure of CSOs to digital security threats, this study aims to achieve the following objectives:

1. Identify and analyse the most common digital security threats that CSOs in West Africa encounter.
2. Assess the level of exposure of CSOs to digital security threats and attacks.
3. Evaluate the level of preparedness of CSOs in responding to digital security threats and attacks.
4. Examine national-level policies in West Africa to address digital security.
5. Examine organisational-level digital security policies among CSOs in West Africa.
6. Identify the major challenges that hinder the ability of CSOs in West Africa to effectively manage digital security threats.

The study endeavours to provide valuable insights into the digital security landscape in West Africa and offer guidance for the development of digital security policies that cater to the needs of CSOs in the region.

Methodology

The study uses a comprehensive research design that incorporates both desk-based research and primary data collection techniques. The desk research involves a thorough review of the existing digital security literature and an analysis of the national-level ICT policies in the West African region. A survey approach and key informant interviews are employed to gather primary data. The survey questionnaire was structured in both English and French and had 10 modules covering various relevant themes such as most common digital threats, digital challenges and dangers confronting CSOs, organisational level digital policies, among others.

The sample size of the survey comprised of 284 CSO representatives drawn from a pool of over 2000 CSOs from all fifteen Economic Community of West African States (ECOWAS) countries, plus Cameroon, Chad and Mauritania. These representatives were contacted via email and presented with the questionnaire. Prior to the administration of the main survey, the questionnaire was tested in a pilot study of 20 CSOs in November 2022. The feedback from the pilot study was used to update the questionnaire, which was administered from November 2022 to mid-January 2023. Respondents completed the survey within an average of 13 minutes. The collected data from the survey was used to select key informants for in-depth interviews, which helped to obtain further information about experienced digital security attacks or threats. Table A1 (in Appendix) shows a description of the survey respondents. Overall, 69.29% of the respondents were male, while 30.36% were female, and

54.95% were in senior executive or top-level management positions. In terms of education, 56.79% of the respondents had tertiary or university education. The respondents represented their CSOs from the various West African countries, with Nigeria having the highest representation (32.62%). Also, CSOs engaged in human rights activities were the most represented (54.84%).

Between November 2022 and January 2023, the study conducted Key Informant Interviews (KIIs) with 24 respondents selected from a list of over 60 CSOs that reported experiencing digital security attacks within the last 12 months. The KIIs were conducted electronically or by phone in English or French. Table A2 provides important insights into the Key Informant Interviewees (KIIs), including their gender, education, position, country, CSO classification, and CSO type. The table shows that most of the Key Informants were male (22 out of 24), and they held various positions within the CSOs, including executive directors, project coordinators, and finance and administrative managers. Majority of the interviewees had tertiary/postgraduate education (20 out of 24), and they represented various West African countries including Benin, Côte d'Ivoire, Ghana, Liberia, and Nigeria. Local non-governmental organisations were the most represented CSO classification, with 8 out of 24 interviewees belonging to this category.

The table indicates that human rights CSOs (including organisations protecting the rights of women, children, and minorities) were again the most represented CSO type per thematic area, during the interview phase, with 11 out of 24 interviewees belonging to this category. The KIIs covered various CSO activities, including conflict, peace and security, poverty and hunger, and education, showing the diversity of CSOs that participated in the study, enabling the study to provide a comprehensive analysis of the digital security landscape among CSOs in West Africa.

Key Findings

Key findings from the study include the following:

1. 31% of CSOs in West Africa experienced a digital security attack in the last year.
2. Nigeria had the highest percentage of attacks at 10.75%, with Ghana following closely behind.
3. 25% of attacks happened multiple times in a year.
4. CBOs and LNGOs experience higher rates of attacks compared to INGOs.
5. Majority of CSOs lack proper knowledge and training on how to protect themselves from digital threats and attacks.
6. Limited financial resources prevent many CSOs from allocating a budget for information security.
7. Most CSOs lack preparedness towards responding to digital security threats and attacks.
8. 45% of CSOs are unaware of national

laws and regulations on digital security.

9. Only a small portion of CSOs (23.6%) have computer and information security policies in place, and even among those who have one, many do not fully understand its contents and have been known to deviate from it.
10. CSOs in West Africa face a multitude of digital security challenges that threaten to undermine their efforts in pursuing their mandates. These include in addition to the above mentioned, inadequate ICT and digital security infrastructure.

The findings of this report are ground-breaking in both theoretical and empirical terms as there are very few studies that focus on this topic within the region. The study highlights the urgent need for CSOs in West Africa to invest in digital security education and training, as well as the need for better education and awareness efforts on national laws and regulations on digital security. It also emphasises the importance of having robust digital security laws and policies in place, a harmonised approach to digital security laws and policies across West Africa, and stronger security measures and guidelines for digital security within organisations. The study suggests that targeted training programmes can improve CSOs' overall preparedness, while investments in technology and personnel and the implementation of comprehensive digital security policies and training programmes can keep pace with the rapidly changing digital security landscape.

Outline of the Report

The report is divided into seven main chapters, each addressing various aspects of digital security, from the major digital security threats that CSOs face, to the gaps in existing national policies and laws on digital security.

The introduction highlights the objectives and context of the study, while the second chapter focuses on the major digital security threats confronting CSOs, their frequency, the types of CSOs affected, and geographical distribution. The third chapter describes the nature of digital security activities and technologies adopted by CSOs, their budgetary allocation for digital security, concerns with online operations, and level of exposure to digital security threats and attacks. The fourth chapter evaluates the level of preparedness of CSOs in responding to digital security threats and attacks, while the fifth chapter examines existing national-level laws and policies on digital security in West Africa. The sixth chapter focuses on the organisational-level digital security policies and strategies implemented by CSOs, and the challenges faced in ensuring digital safety. The report concludes by emphasising the significance of digital technologies for the operations of CSOs in the West Africa region, the prevalent digital security threats faced, and makes recommendations for practical applications of digital security for CSOs.

Chapter 2

THE MOST COMMON DIGITAL SECURITY THREATS FACING CSOs IN WEST AFRICA

This chapter focuses on the most common digital security threats faced by CSOs in West Africa. It takes an in-depth look at the major threats, their frequency of occurrence, the types of CSOs that face these threats, the relationship between the perceived level of digital security and the age of the organisation, and the geographical distribution of digital security threats/attacks.

Key Insights

31%

of the sampled CSOs have **experienced** a digital security attack within the last twelve months.

48%

of CSOs that have fallen victim to attacks, have experienced **computer virus** attacks that harmed data.

35%

Nigeria accounts for over a third of the experienced attacks (35%) followed by Ghana (17%), Cote d'Ivoire (8%) and Guinea (8%).

CSOs' Digital Security Experience over the past 12 months

The increasing prevalence of digital threats and attacks among organisations and individuals has led to expert advice on securing digital networks against breaches. While technical expertise is important, there are other factors such as good managerial conduct and effective legal and policy strategies that are necessary to address digital security threats. Failure to create these enablers implies the persistent occurrence of common digital security threats among CSOs, as highlighted by previous studies (Adomako et al., 2018; Bohme, 2005). In line with these findings, the survey data from this study shows that nearly one-third (31%) of the sampled CSOs have experienced a digital security attack within the last twelve months, indicating that digital security threats are a significant concern for CSOs in the region, as shown in Figure 1.

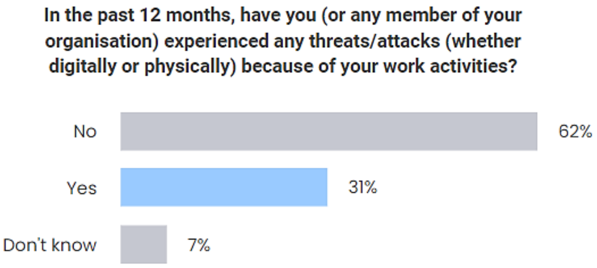


Figure 1: CSOs' Digital Security Experience over the past 12 Months / Source: WACSI (2023)

The high rate of attacks among the sampled CSOs highlights the prevalence of digital security threats in the West Africa region and underscores the urgent need for better digital security practices, policies, and training programmes to mitigate these risks.

Types of Digital Security Threats/Attacks Experienced among CSOs

Digital threats come in all shapes and sizes, as Quarshie, & Martin-Odoom (2012) uncovered. From data hacks to scams, confiscation of devices to fraudulent activities, these virtual dangers are not to be underestimated. This study delves into these different facets of digital threats and presents its findings in Figure 2. The blue bars represent the threats/attacks as a percentage of all survey respondents whereas the yellow bars show the results as a share of experienced attacks.

The data revealed in Figure 2 paints a dire picture for CSOs in West Africa. Most of the victims experienced multiple cases, with 48% of them experiencing virus attacks, 43% experiencing social media attacks and 33% being attacked via emails. This highlights the rampant presence of malware and phishing in the region. But it is not just virtual threats that CSOs must worry about. Some 26% reported physical attacks, while 25% had their publication, website or blog hacked. The dangers of online surveillance and impersonation were also reported by 24% of the CSOs. Additionally, 9% reported that their friends or family were threatened, 9% experienced email interception, 9% were targeted by an online disinform campaign, and 9% were illegally arrested.

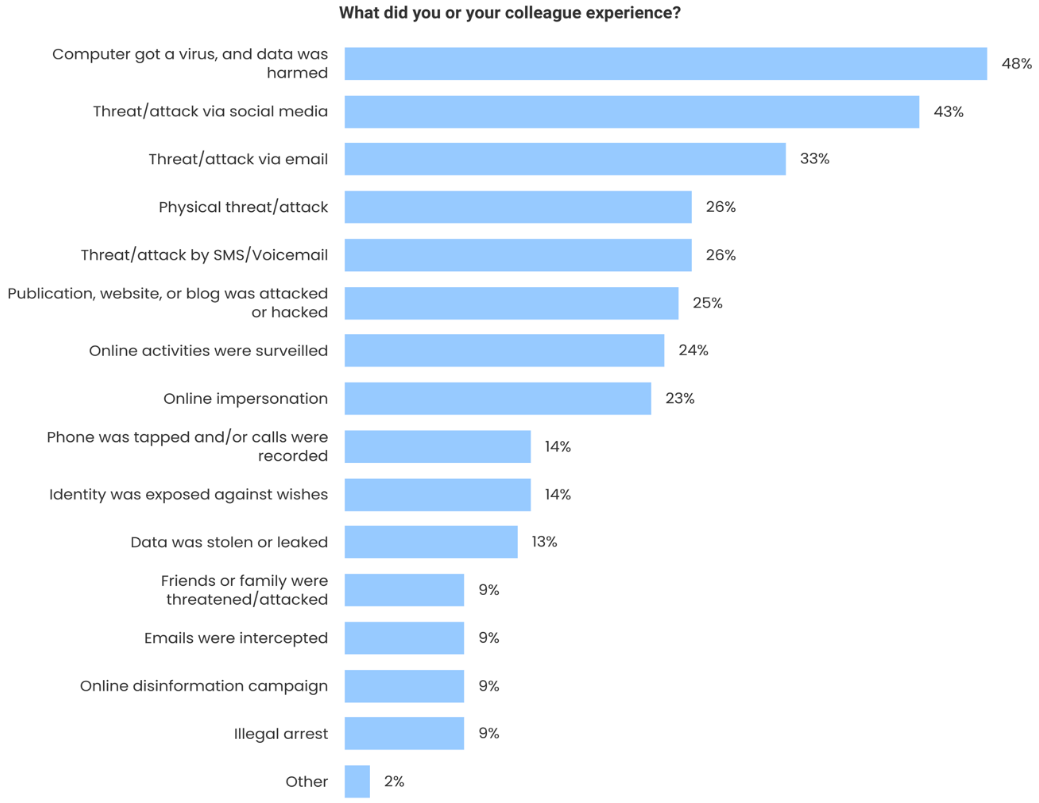


Figure 2: Types of Digital Security Experienced Among CSOs / Source: WACSI (2023)

The survey results suggest that CSOs in West Africa are facing a multifaceted threat landscape, including hacking, surveillance, impersonation, and even targeted attacks aimed at silencing or intimidating them. Nearly half of experienced attacks are computer malware or virus attacks that resulted in data loss. Phishing attacks particularly through social media and emails, hacking, physical or targeted attacks are also prominent. In some instances, CSOs experience multiple threats or attacks. Box 2.1 presents the case of a CSO based in Nigeria that experienced several digital security incidents.

Box 2. 1: The "Double Hit" / Source of excerpt: KII20

CASE STUDY

This case study describes a number of digital security incidents experienced by a CSO in Nigeria that is into leadership training of young people. Specifically, the attacks are in the areas of website security and social media account security.

I am the regional communication officer, and I also double as the IT personnel handling everything technical and digital, including graphic design and website management. I will start with the website since it is where we first noticed changes. I built the website on a web-based platform and noticed some pages were not functioning well. When I complained to the host company, they told me that the SSL certificate had expired and needed to be renewed. I explained that we had paid for the certificate 2-3 years ahead, and they apologized for not seeing the invoice, refunded the money, and took down the certificate. I suspect this was when the attack happened. Currently, about 80% of the site is not functioning, and when you click on some pages, it closes and gives a 404 error message. We discovered that attackers had been able to access the back end and inject the site with malware, causing some codes I did not put there to appear. Currently, the attackers have taken down the main site and two sub-domains, and I need to remove the malware manually.

The second incident involved the suspension of the organisation's Facebook account on December 3, 2022. When I tried to log in to Facebook to make a post, I was told the account was suspended. When I tried to log in to Instagram, I was told that the account was also suspended because it was linked to the Facebook account. On checking, I saw that Facebook had found the account to be non-compliant with community guidelines. I hardly used the account, and it was created years before

I joined the organisation, primarily for creating Facebook posts, and therefore, had no personal identification. We only used it for the pages and had no government-issued identification for the account. I had to submit the CAC certificate used to register our organisation, but the documents were rejected, so I had to tell them that my account was hacked, and I did not know what happened. They asked me to change my password, and they would get back to me after reviewing the documents. I have not heard back from them since. We have had to create another account and start from scratch, including Instagram, hoping that Facebook will restore the old account. It was a double hit experience.

The first incident described is an issue with the SSL certificate on the organisation's website, which caused some pages to not function properly and resulted in the host company having to apologize and refund the organisation. This suggests that there may have been an issue with the host company not properly renewing or maintaining the SSL certificate, potentially leaving the website vulnerable to attacks.

The second incident described is a malware attack on the organisation's website, which resulted in some code being injected into the site that was not put there by the organisation. This suggests that the attackers were able to gain access to the back end of the website, potentially through a security vulnerability or by exploiting a weakness in the organisation's digital security practices.

The third incident described is the suspension of the organisation's Facebook account due to a violation of community guidelines. The interviewee suggests that this may have been the result of an account hack, but it is not clear what specifically led to the account being suspended. This incident highlights the importance of having proper identification and documentation for social media accounts, as well as regularly monitoring and securing these accounts to prevent unauthorised access.

Overall, the incidents described in this case study suggest that the organisation had weaknesses in its digital security practices, particularly in the areas of website security and social media account security. Other CSOs in West Africa can learn from this experience by ensuring that they properly maintain and renew SSL certificates for their websites, regularly monitor and secure their social media accounts, and have proper identification and documentation for those accounts in case of suspension or other issues. Lastly, they should have a regular process of monitoring their website and social media accounts for any suspicious activities or unusual changes.

Anderson (2001) had a keen eye for the root cause of digital security threats - outdated technology, lack of investment, insufficient awareness, and human error. Unfortunately, many CSOs in West Africa remain blind to the importance of investing in secure technology for their online operations, as they fail to see the direct correlation between digital security and their core interests and operations. The result? A digital world of CSOs vulnerable to the consequences of their apathy.

Geographical distribution of digital security attacks/threats

The digital world is constantly evolving, and with it, the threats and attacks faced by organisations. The survey reveals that the percentage of experienced digital security threats varies greatly among different countries in West Africa, with Nigeria leading with 10.75% and Ghana following close behind at 5.38%. However, it is important to note that the absence of reported threats in countries like Guinea-Bissau, Mauritania, and Senegal should not be taken as an indicator of immunity. In fact, these countries are also the least represented in the data, which does not make it less crucial in those countries. The digital world may be full of opportunities, but it's also rife with danger, and it's imperative that CSOs stay ahead of the curve.

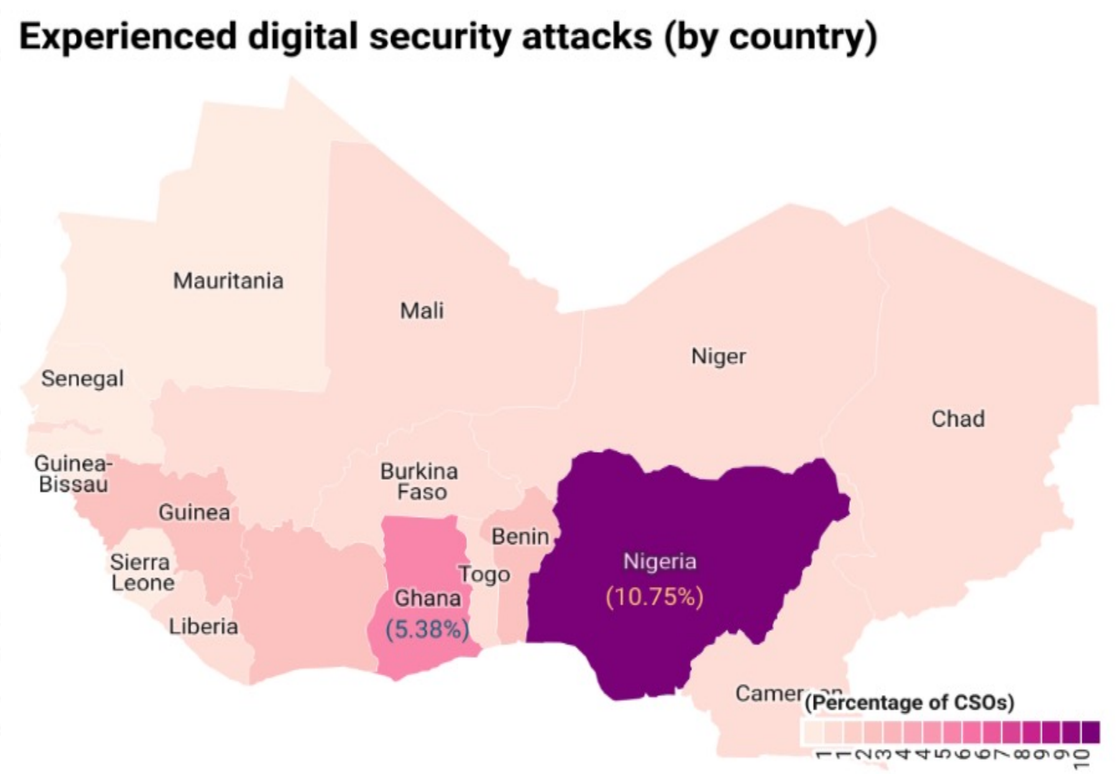
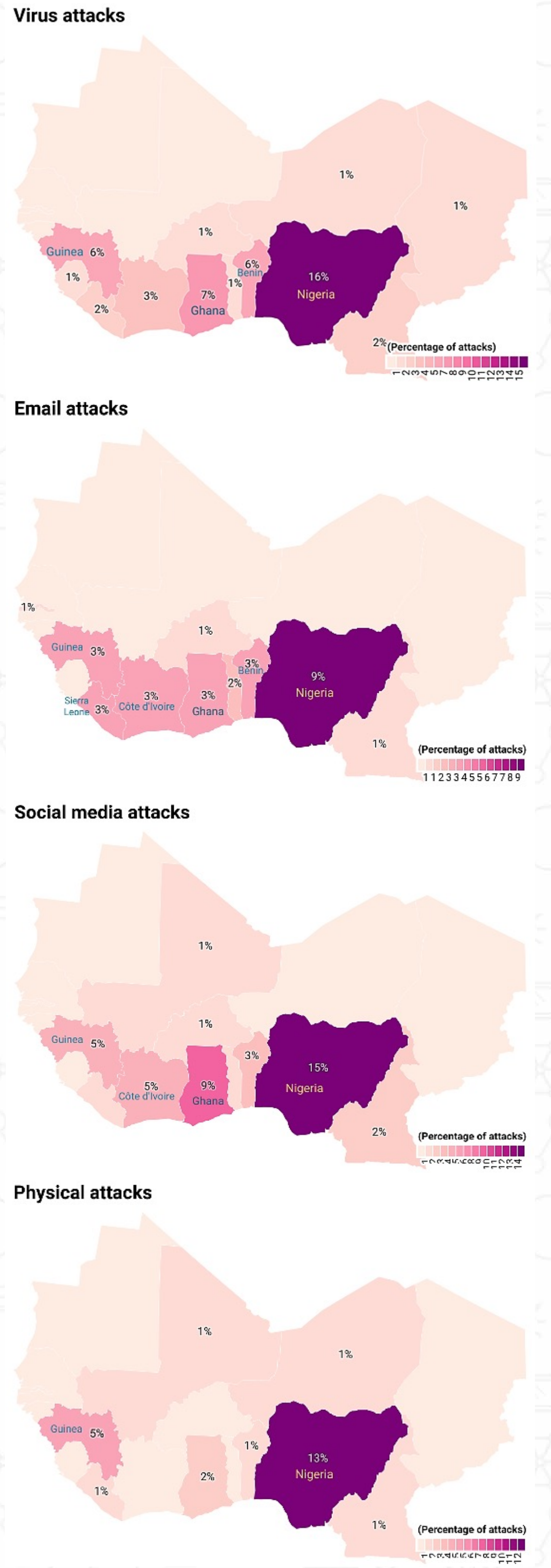


Figure 3: Experienced attacks by country / Source: WACSI (2023)



Virus attacks

Email attacks

Social media attacks

Physical attacks

Figure 4: Geographical distribution of top four digital security attacks or threats / Source: WACSI (2023)

Nigeria has the highest percentage of virus attacks at 16.28%, followed by Ghana at 6.98% and Cote d'Ivoire at 3.49%. The remaining countries have a relatively low percentage of reported virus attacks, with some countries such as Senegal and The Gambia reporting no experienced attacks at all.

Nigeria again has the highest percentage of email attacks at 9.30%, followed by Guinea, Cote d'Ivoire and Liberia at 3.49%. The remaining countries have a relatively low percentage of reported email attacks, with some countries such as Senegal and The Gambia reporting no experienced attacks at all.

For social media attacks, Nigeria again has the highest percentage at 15.12%, followed by Ghana at 9.30% and Côte d'Ivoire at 4.65%. Chad, Senegal and The Gambia reported no experienced social media attacks.

Regarding physical attacks, Nigeria again has the highest percentage at 12.79%, followed by Guinea at 4.65% and Ghana at 2.33%. Again, the remaining countries have a relatively low percentage of reported physical attacks, with some countries such as Senegal and The Gambia reporting no experienced attacks at all.

Overall, it appears that Nigeria has the highest rate of experienced digital security threats and attacks among the countries in West Africa, followed by Ghana and Côte d'Ivoire. The remaining countries have relatively low percentages of reported attacks.

However, as indicated above, it is important to note that this data is based on self-reported survey results and may not represent the full scope of digital security threats and attacks in these countries.

In addition, our sample is not nationally representative. Nevertheless, the implications of these findings are far-reaching and call for action on multiple fronts. Firstly, the governments in these countries, particularly Nigeria, need to step up their game and enhance their digital security measures. CSOs must also be proactive in securing themselves against potential attacks.

The private sector in these countries cannot afford to be complacent either, they must take an active role in ensuring the digital security of their operations.

Frequency of Occurrence of Digital Threats among CSOs

Understanding the frequency of digital security threats and attacks among CSOs in West Africa is of utmost importance as it helps organisations to better prepare and prevent future threats, allocate resources effectively, raise awareness, respond more effectively when an attack occurs, and make informed decisions regarding digital security.

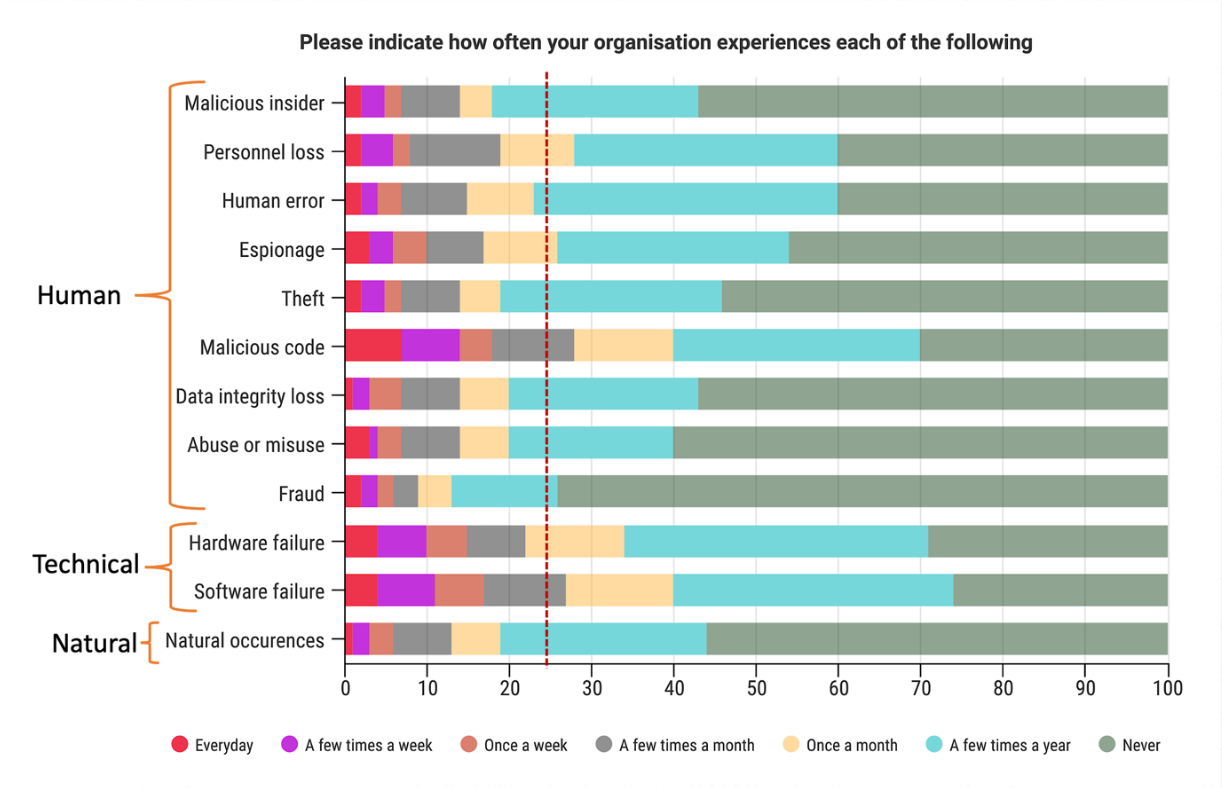
This information provides a basis for evidence-based decision-making and allows organisations to prioritise their security needs. By knowing the types of attacks that are most common, organisations can take proactive measures to protect their digital assets, thereby improving the digital security landscape in the region and ensuring the protection of sensitive information and assets.

The attacks can be grouped according to human, technical and natural sources, and they are presented in this section by their technical names.

For example, the human sources include malicious insider, personnel loss, human error, espionage, theft, malicious code, data integrity loss, abuse or misuse and fraud.

The technical sources include software and hardware failure, whereas the natural sources consist of fire, water or extreme weather conditions that cause digital device or system malfunction.

The frequency of occurrence of these attacks is first analysed altogether using Figure 5 (a & b) before examining them one by one and describing them in detail.



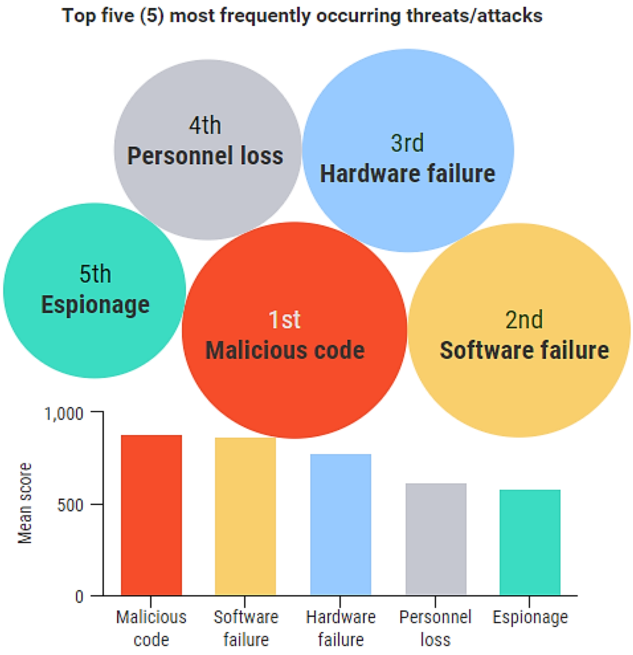


Figure 5: Frequency of Occurrence of Digital Threats among CSOs / Source: WACSI (2023)

The results presented in Figure 5a show that roughly over a fifth (1/5) of CSOs experience attacks on a regular basis, ranging from every day to a several times a month.

Interestingly, by weighing and aggregating the scores in Figure 5, malicious code, software, hardware failure, personnel loss, and espionage appear to be the top five most frequently occurring threats or attacks as shown by Figure 5b.

Human error, theft, malicious insider, data integrity loss, abuse or misuse, natural occurences and fraud complete the order; the next session takes a closer look at each.

Frequency of attacks caused by humans

1. Malicious code

A malicious code, also known as malware, is a software programme with malicious intent. With 30% of the CSOs experiencing attacks from malicious codes several times a year and 7% being hit every day, this threat is perhaps the most frequently occurring (see Figure 6) among CSOs in West Africa. Interestingly, Humayun et al. (2020), after reviewing 78 primary studies from 2007 to 2018 across several countries, found malware to be one of the (top two) most common digital security attacks. Malware can spread through email attachments, infected websites, or other means of delivery and can perform a range of actions, such as stealing sensitive information, encrypting files for ransom, and even taking control of the infected machine.

From viruses and worms to Trojans, ransomware, adware, rootkits, and spyware, the different types of malware pose a significant risk to organisations. As Humayun et al. (2020) note, the motivations for launching malware attacks could include financial and political incentives. CSOs in West Africa need to implement robust security measures to combat this widespread threat. Box 2.7 (in Appendix 2) presents the case of a malware attack experienced by a CSO in Ghana.

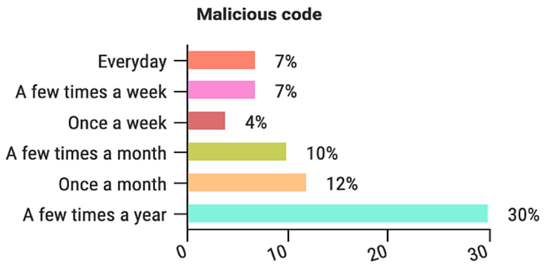


Figure 6: Malicious Code Digital Threat / Source: WACSI (2023)

2. Personnel loss

Figure 7 and Box 2.2 (in Appendix 2) show that losing personnel can be a major risk for CSOs in West Africa, as it opens the door for potential harm to the organisation. According to survey results, 32% of the respondents reported experiencing personnel loss several times a year, with 11% recording it several times a month. Whether it's due to an employee's temporary absence, departure, or leave of absence, the absence of key personnel can lead to the loss of sensitive information and the disruption of operations. In some cases, an employee may have been responsible for digital security responsibilities, leaving them unattended during their absence. A personnel loss can also increase the risk of confidential information being leaked or the employee using their knowledge of the organisation to aid a competitor. The key lesson here is for CSOs to be proactive in addressing personnel loss and protecting against potential threats.

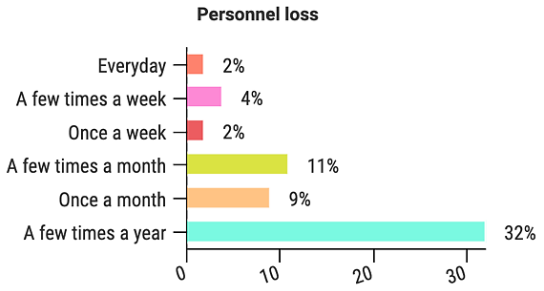


Figure 7: Personnel Loss Digital Attack / Source: WACSI (2023)

3. Man-in-the-middle (MitM) attacks

A MitM is another common attack where the perpetrators or their technologies occupy the link between a victim and a target website. In the process of the MitM attack, the perpetrator can secretly extract information from both ends and can even vary the content without the victims' knowledge. A common form of MitM attack is where the attacker uses a WiFi router to monitor conversations. That is, the attacker sets up a wireless device to serve as a WiFi hotspot and gives it a common name within a public setting to lure people to trust the legitimacy of the connection. People then click to connect and visit sites where they enter their email login credentials or email account details. These account details are stored on the site for the attacker to use later (Fisher, 2013). The motivation for MitM attacks could range from damaging trust and communications, spying on individuals' communication to moving money from the victim's account (McDowell, 2013). One form of MitM attack is espionage.Bottom of Form Espionage looms as a formidable threat to CSOs in West Africa, with 28% of those surveyed reporting experiencing this underhanded tactic several times a year. Espionage involves surreptitiously gathering information or intelligence about an organisation without its knowledge or consent, with the purpose of gaining political, economic, or other forms of advantages, or sabotaging the organisation's operations. Cyber-espionage is one form of this threat, using digital tools to extract information from an organisation's computer systems or networks. Human-based espionage uses human agents to gather information, while physical surveillance employs cameras, bugs, or other devices to monitor an organisation's activities. Social engineering also poses a risk, where psychological manipulation is used to trick individuals into revealing sensitive information. The impacts of espionage can be far-reaching and devastating for CSOs such as, loss of funding from partners and donors, and legal liabilities.

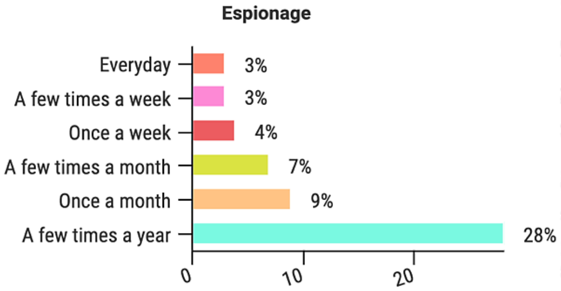


Figure 8: Espionage Digital Security Attack / Source: WACSI (2023)

4. Phishing campaigns

CSOs and other advocacy organisations are vulnerable to surveillance through phishing and spearphishing campaigns. These malicious attacks usually involve sending emails or links loaded with viruses via social media platforms or email (Galperin and Marquis-Boire, 2012). Of all the viruses, the most destructive and widespread is the Remote Access Trojan (RAT). The higher the RAT's sophistication, the higher the chances of it going undetected by anti-virus software. In some cases, these attacks are launched on fake websites, tricking individuals into entering their account information which is then extracted without their knowledge. A common phishing attack is when CSOs receive fraudulent emails that appear to be from a familiar source or someone they know, luring them into clicking on a link or downloading an attachment that infects their computer with viruses. To significantly reduce the occurrence of these attacks by 85% or more, it is important for CSOs to avoid accessing attachments directly (Rights Con, 2014). Box 2.5 (in Appendix 2) presents the case of a CSO in Ghana that fell victim to a phishing campaign, stressing the need for CSOs to be vigilant in order to avoid this type of attack.

5. Malicious insider attack

A quarter (1/4) of the CSOs who were attacked have experienced malicious insider attacks multiple times a year, with 7% reporting monthly occurrences. These attacks come from current or former employees, contractors, or others who have been trusted with access to sensitive information or systems but have taken advantage of that trust for their own illegal or unauthorised purposes. The impact of these attacks can be devastating, as they compromise the integrity and trust of the organisation, putting sensitive information at risk, and can harm their reputation, relationships and work. The consequences of a malicious insider can range from sharing confidential information, unauthorised access to data, to even sabotaging operations.

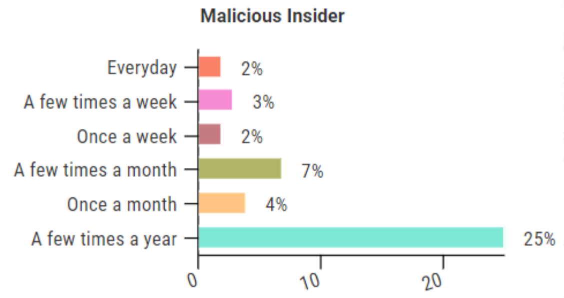


Figure 9: Malicious Insider Online Attack / Source: WACSI (2023)

6. Human Error

Human error is a digital security threat that occurs when an organisation's staff members, intentionally or unintentionally, cause damage to the organisation's digital assets. This can take several forms, such as malicious insiders who actively seek to harm the organisation, employees who fall victim to social engineering attacks, staff members who inadvertently introduce malware to the organisation's network or those who inadvertently cause data breaches through their actions. For example, a staff member who falls for a phishing email and reveals sensitive information; a disgruntled employee who intentionally shares confidential data; an employee who unknowingly downloads malware from the internet; or a staff member who leaves the organisation and takes sensitive information with them. Figure 8 shows that over a third of the CSOs (37%) who experienced attacks recorded human errors several times a year. Box 2.3 (in Appendix 2) describes an example of a human error experienced by a CSO in Ghana. Respondent KII13 narrates their CSO's vulnerability and experience of human error attack in Ghana.

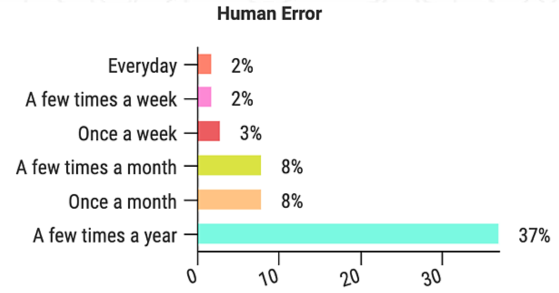


Figure 10: Human Error Digital Threat / Source: WACSI (2023)

7. Theft

Theft strikes at the heart of the CSOs, with 27% reporting multiple incidents of theft each year and 7% falling victim monthly, according to the data in Figure 11. Theft encompasses the illegal access, use, exposure, destruction, or acquisition of confidential information or assets belonging to the CSOs. This type of digital threat can take on many forms, including hacking, where a malicious individual gains unauthorised access to a computer system through malicious software or social engineering techniques; phishing, where scammers trick people into revealing sensitive information through emails, phone calls, or text messages; insider threat, where a trusted employee, contractor, or other individual with access to the CSOs' information and systems steal sensitive information; data breaches, where sensitive information is exposed due to security vulnerabilities in a system or application; ransomware, a type of malware that demands payment in exchange for unlocking encrypted data; advanced persistent threat, where a highly-skilled and well-resourced attacker, often a nation-state, steals sensitive information over a prolonged period of time; industrial espionage, where rival organisations or governments steal sensitive information or assets. These types of digital security threats can result in data loss, operational disruptions, and financial damage, which is why it is crucial for CSOs to implement strong security measures to prevent theft.
Confiscation of physical digital devices, such as mobile phones, laptops, and data storage devices, also pose a threat to CSOs' confidential communications. These devices contain valuable information, including the names and contact information of partners and employees, financial reports, and other sensitive data, which can put people's lives at risk if exposed (Aikins, 2012). An example of an experience of this attack is narrated by respondent (KII18 and KII5) in Box 2.6 (in Appendix 2).

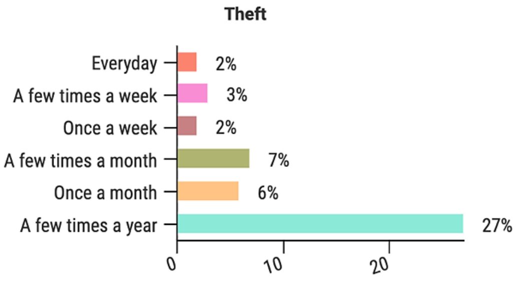


Figure 11: Theft Digital Threat / Source: WACSI (2023)

8. Data integrity loss

For West African CSOs, data integrity loss is a frequent occurrence. Nearly a quarter of respondents (23%) experience this type of digital security threat several times a year, with 7% experiencing it monthly. This type of attack is characterised by the compromise of the authenticity, completeness, and reliability of data stored in a computer system, and it can happen in a variety of ways. For instance, a hacker could gain access to a CSO's database and manipulate sensitive information, causing it to become unreliable This can also be caused by malicious insiders who deliberately alter or delete important data. Even simple human error, such as accidentally deleting important files or not properly saving changes, can lead to data integrity loss. Regardless of the cause, this type of attack puts the mission of CSOs at risk and can also lead to serious consequences, such as loss of funding from partners and donors and potential legal liabilities. Box 2.4 (in Appendix 2) describes how a hacking incident experienced by a CSO resulted in the posting of inappropriate content on the CSO's social media account that devastatingly tarnished the image of the organisation.

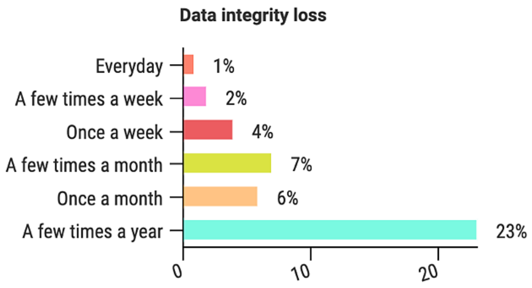


Figure 12: Data Integrity Loss Digital Threat / Source: WACSI (2023)

9. Abuse or misuse of digital device or system

A fifth (20%) of the CSOs experience abuse or misuse of digital devices, multiple times a year, with 7% experiencing it several times a month, as shown by Figure 13. Abuse or misuse refers to the unauthorised or inappropriate use of digital resources by employees, partners, or other individuals. Examples of abuse or misuse include sending personal emails or browsing non-work-related websites on organisational devices or using organisational resources for personal gain, accessing sensitive data without authorisation, or sharing of sensitive information with unauthorised parties. This kind of threat may cause reputational, legal, or financial damage to the CSOs and compromise the integrity of the data and information they hold. Having proper access controls, monitoring, and incident response plans in place can help prevent and detect such misuse and abuse.

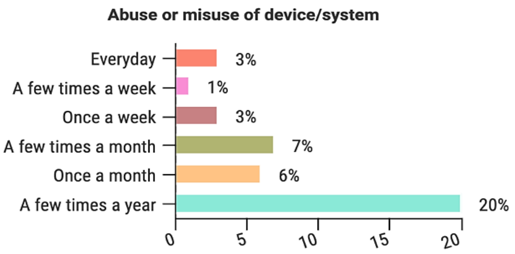


Figure 13: Abuse or misuse of device/sytem / Source: WACSI (2023)

10. Deceptive domain attacks

Deceptive domain attacks come in two forms: infecting computer systems with viruses and creating false content on fake websites that threaten the credibility of the CSO. In the latter scenario, the attacker creates a website that appears identical to the target CSO's site, and completes it with replicated content, to lure visitors to the fake site where they will be infected with viruses. These attackers also expand their reach by creating fake social media accounts linked to the fake website in a bid to outrank the real site and attract even more visitors (Access, 2014). The ultimate goal of a fake domain attack can range from diverting information, stealing the information of visitors, or altering the public's perception of the CSO (Access, 2014). Although this study does not report the frequency of fake domain attacks, a study by Access (ibid) reveals that over a 10-month period, fake domain attacks accounted for 4% of 60 unique cases. Box 2.8 (in Appendix 2) presents the case of how a deceptive domain was used to plot a scam on an organisation.

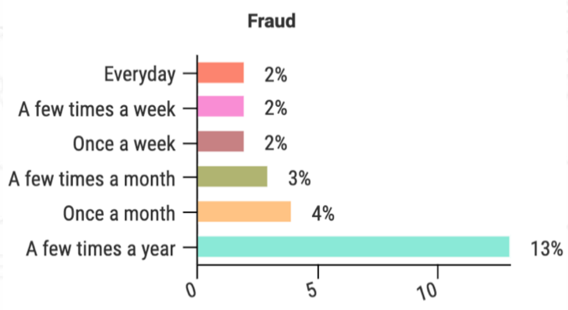


Figure 14: Fraud Digital Security Threat / Source: WACSI (2023)

11. Fraud

Fraudulent schemes are also on the rise, targeting unsuspecting CSOs in West Africa with devastating consequences. About 13% of the CSOs report experiencing this deceitful tactic several times a year, resulting in financial loss and reputational damage. Embezzlement, phishing scams, and impersonation are just a few examples of the cunning methods used by perpetrators to manipulate and mislead organisations. Despite efforts to implement digital safety measures, these attacks often prove too slick for even the best-laid plans.

Other human sources of digital security attacks

There are other shadows of digital danger cast by human hands, not captured in this study in terms of their frequency of occurrence but they are never to be underestimated. From the depths of the online world, these threats emerge to haunt CSOs in West Africa. Intimidation and harassment, filtering of content, and even malicious manipulation on social networking sites, outlined in Boxes 2.9 and 2.10 (in Appendix 2), are some of the experiences that have been reported. The current state of the literature on these attacks are provided below to give an overview of their prevalence in West Africa.

1. Intimidation, harassment and forced exposure of online networks

Employees are facing a barrage of attacks ranging from harassment and intimidation to blackmail and arrest. The International News Safety Institute (2014) reported that multiple forms of these attacks are becoming increasingly common. Tragically, the Committee to Protect Journalists (2014) found that 38% of employees from CSOs and other media organisations received threats before their murder in the last two decades. The physical attacks on employees from advocacy groups are on the rise, with some facing online threats, others being murdered, and some even tracked down through their mobile phones, coerced to release digital account information, and physically assaulted (Henrichsen et al., 2015). This trend is a dire threat to the safety and security of CSO employees. Box 2.9 presents a case from this study where an employee of a CSO experienced extortion and harassment attacks from social media to the physical realm.

2. Filtering

In the Middle East, North Africa, and West Africa, censorship by governments is all too real for CSOs and non-state actors. Freedom of speech is stifled by limited access to stable internet, and as internet access expands in Africa, countries like Ethiopia and The Gambia are taking steps to censor websites and restrict access (Henrichsen et al., 2015). Filtering is the process of blocking, limiting, or restricting access to certain websites, information, or content on the internet. This can be for various reasons, such as censorship laws, protecting children from harmful content, or preventing illegal material. Filtering can be carried out by government agencies, internet service providers, schools, or other organisations, and it is a threat to digital security because it limits access to information and restricts communication and information sharing online. More on the repressiveness or progressiveness of the civic space through filtering in West Africa can be found in Chapter five.

3. Social networking sites

Social media networks are the new playground for creating and maintaining friendships, but at what cost to privacy? With each site requiring users to share their information, including interests, location, and date of birth, the sensitive details of millions of users are readily accessible. Privacy violations have become a growing concern as attackers extract information from these platforms to launch malicious attacks through blackmail or account hacking. The easy targets are often users who freely share their personal information on these sites, leaving them vulnerable (Citizen Lab, 2013). Box 2.10 describes a case where the personal information of the informant's sister was extracted from an online platform without her knowledge, and used for a scandalous purpose.

Frequency of attacks caused by technical failures

1. Software failure

Software failures are considered a technical failure because they are caused by the malfunctioning of computer systems and software. This may occur due to a variety of reasons such as bugs in the code, compatibility issues, or software design flaws. Unlike human errors, which are caused by individuals, software failures are not directly caused by human actions but by the underlying technology. Hence, they are typically referred to as technical failures rather than human-caused failures.

The survey data shows that software failure is one of the most common or frequently occurring digital security threats facing CSOs in West Africa, with 34% experiencing it several times a year and 10% experiencing it multiple times a month. Although software malfunctions may result from bugs in the software, conflicts with other software, or even hardware failures, the installation of fake or pirated software, lack of system updates or maintenance, improper installation, and data corruption or loss among CSOs significantly increase the scale and potential of the harm. Apart from these, software failure could also be a result of a vulnerability or weakness in the software system, or due to malicious attacks such as hacking or malware infection.

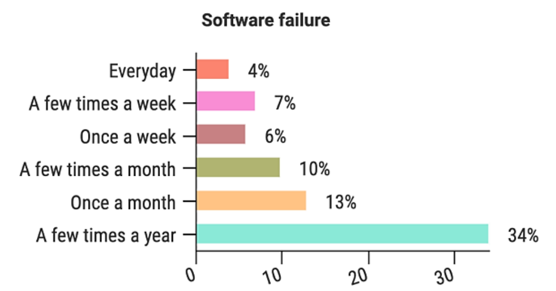


Figure 15: Software Digital Threat / Source: WACSI (2023)

2. Hardware failure

Hardware failure also refers to the malfunction or breakdown of physical equipment and devices used by the organisation. This can include computers, servers, printers, routers, and other types of hardware. Hardware failure is also one of the most frequently occurring threats among the CSOs in West Africa on a yearly basis. The survey data shows that 37% of the CSOs experience it several times a year, with 12% experiencing it once a month. Hardware failure can occur due to a variety of reasons such as wear and tear, overheating, power surges, and other types of physical damage.

The implications of hardware failure for CSOs in West Africa can be significant. For instance, if a server or a computer fails, it can disrupt the organisation's operations, resulting in loss of data, delay in activities, and a lack of communication with partners, stakeholders and beneficiaries. Additionally, hardware failure can cause financial losses as the organisation may have to repair or replace the damaged equipment.

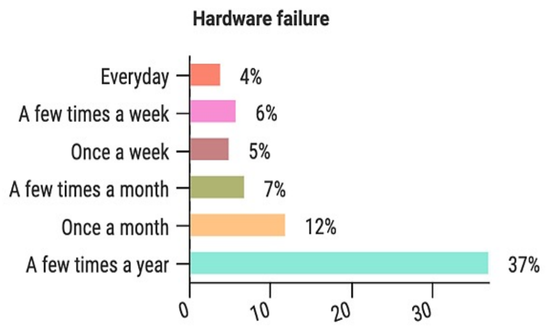


Figure 16: Hardware Digital Threat / Source: WACSI (2023)

Frequency of attacks caused by nature

Natural Threats/Attacks

A shocking 25% of the CSOs reported experiencing attacks from Mother Nature several times a year, with 7% hit multiple times a month. Natural disasters can wreak havoc on the organisation's infrastructure, causing physical damage to servers and equipment, disrupting power and internet connectivity, and making it impossible for staff to access essential information. From devastating floods to harsh weather conditions, these events leave devastating impacts on organisations, leading to operational disruptions, data and financial loss.

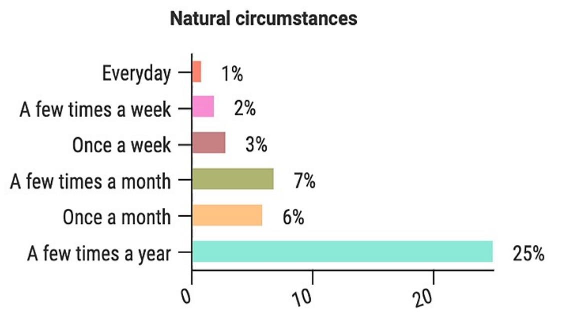


Figure 17: Natural Citrcumstances Digital Threat / Source: WACSI (2023)

Variation in Digital Security Incidents across Types of Organisations

It's fascinating to note that different types of CSOs face unique digital security incidents. Some attacks are more common among certain types of CSOs than others. The study highlights the various types of CSOs, including Community-Based Organisations (CBOs), Local Non-Governmental Organisations, International Non-Governmental Organisations (INGOs), and the specific digital threats they encounter (as shown in Figure 18 and Table 2).

The results in Table 2 (and Figure 18) show that overall, INGOs experienced the lowest rates of attacks.

To cite a few examples; for computer getting a virus and data being harmed, LNGOs and other CSOs have the highest reported rate at 33%. Other CSOs also have the highest rates of attack in the case of social media attacks (31. 6%) and email attacks (39.3%).

In terms of illegal arrest, and friends or family being threatened/attacked, CBOs suffered the most (44.44% and 57.14% respectively). LNGOs also have the highest rate of physical attacks (36.36%).

The high rate of illegal arrests for CBOs may indicate that they are more likely to be targeted for their work or activism. It is also worth noting that the overall high incidence rate among CBOs and LNGOs suggests that perhaps they have limited resources as compared to INGOs.

Their limited resources thus may prevent them from adequately anticipating and addressing their digital security issues.

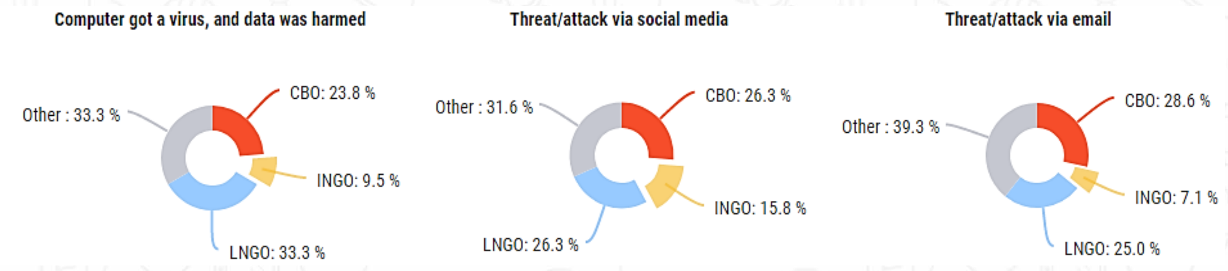


Figure 18: Types of CSO and Experienced Threat/Attack / Source: WACSI (2023)

Table 2: Digital security threats/attacks by CSO Type

	CSO Type				
	CBO	**INGO**	**LNGO**	**Other**	**Total**
Computer got a virus, and data was harmed					
No	22.22	15.56	22.22	40	100
Yes	23.81	9.52	33.33	33.33	100
Illegal arrest					
No	20.51	12.82	26.92	39.74	100
Yes	44.44	11.11	33.33	11.11	100
Physical threat/attack					
No	21.54	13.85	24.62	40	100
Yes	27.27	9.09	36.36	27.27	100
Threat/attack via email					
No	20.34	15.25	28.81	35.59	100
Yes	28.57	7.14	25	39.29	100
Threat/attack by SMS/Voicemail					
No	21.54	13.85	24.62	40	100
Yes	27.27	9.09	36.36	27.27	100
Threat/attack via social media					
No	20.41	10.2	28.57	40.82	100
Yes	26.32	15.79	26.32	31.58	100
Online activities were surveyed					
No	20.59	11.76	30.88	36.76	100
Yes	31.58	15.79	15.79	36.84	100
Friends or family were threatened/attacked					
No	20	12.5	28.75	38.75	100
Yes	57.14	14.29	14.29	14.29	100
Identity was exposed against wishes					
No	20.27	13.51	31.08	35.14	100
Yes	38.46	7.69	7.69	46.15	100
Publication, website, or blog was attacked/hacked					
No	24.62	10.77	27.69	36.92	100
Yes	18.18	18.18	27.27	36.36	100
Emails were intercepted					
No	24.05	13.92	26.58	35.44	100
Yes	12.5	0	37.5	50	100
Data was stolen or leaked					
No	23.08	14.1	28.21	34.62	100
Yes	22.22	0	22.22	55.56	100
Phone was tapped and/or calls were recorded					
No	20	14.67	28	37.33	100
Yes	41.67	0	25	33.33	100
Online impersonation					

No	22.22	14.29	30.16	33.33	100
Yes	20	10	25	45	100
Online disinformation campaign					
No	21.33	13.33	29.33	36	100
Yes	25	12.5	25	37.5	100
Other					
No	22.22	12.35	28.4	37.04	100
Yes	0	50	50	0	100

Source: WACSI (2023)

Nevertheless, the survey results show that overall, all types of organisations are vulnerable to most threats and attacks particularly via email and social media, which highlights the importance of digital security training and practices for all organisations,

CBOs may benefit from accessing anti-virus software, training on how to use it and keep it updated, and educating staff on safe internet practices such as avoiding suspicious emails or downloading unknown files, while LNGOs may need more support in protecting themselves from physical attacks. However, all types of organisations may benefit from guidance on how to protect themselves from email and social media threats.

Perceived digital security level and age of organisation

Considering that different types of organisations experience different digital security incidents, it is possible that organisations become more cyber resilient as they age (or become more established). The study examined how secure respondents think their digital devices are, in their organisation. The respondents were to rate their organisations on a scale of 1 to 10 where 1 indicates very secure and 10 indicates not at all secure. We used this as an indicator of the digital security level of the CSO. We also collected information about the number of years their organisation has been in existence, as a proxy for how established they are. Although these two indicators may have their weaknesses, we plot them on a graph to have an idea of a potential relationship. The results are presented in Figure 19.

Figure 19 suggests that perceived level of digital security among the CSOs is relatively consistent regardless of how long the CSO has been in existence.

The linear fit is flat at 6 on the vertical axis, indicating that the perceived level of digital security does not seem to increase or decrease as the CSO becomes more established. Additionally, the confidence interval widens by years, which suggests that there is more uncertainty or variability in the perceived level of digital security as the CSO becomes more established.

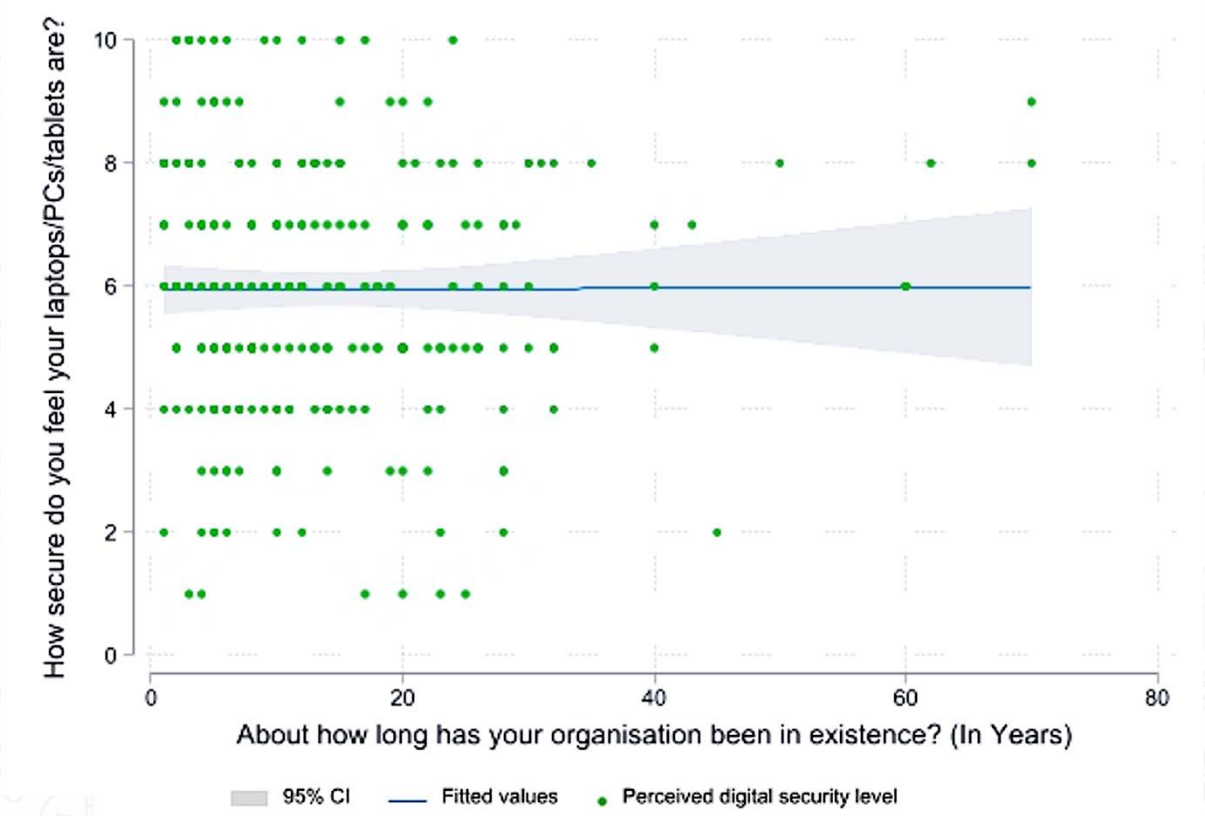


Figure 19: Digital Security and Age of Organisation / Source: WACSI (2023)

One possible implication of this is that it might be wrong to assume that CSOs are prioritising their digital security as they become more established, or are investing in the necessary resources or training to improve their digital security measures. The results could also imply that the CSOs are not generally aware of the potential threats and vulnerabilities that might arise as the organisation grow in size and complexity. It might be useful for future studies to gather additional information to understand why this might be the case.

Chapter 3

EXPOSURE TO DIGITAL SECURITY THREATS AND ATTACKS AMONG CSOs IN WEST AFRICA

This chapter discusses CSOs' exposure to digital security threats and attacks in West Africa. It maps out the nature of digital security activities among CSOs, the technologies they adopt, their key activities of digital safety, their budgetary allocation for digital security, their concerns of operating online, and the extent to which they are exposed to digital security threats and attacks.

Key Insights

99%

of the CSOs use **emails.** Laptops or desktop computers (97%) and mobile phones or tablets (89%) are also widely used.

85%

of the CSOs are **worried about** the safety of **Information** in their organisation.

12%

of the sampled CSOs (only) allocate a **budget** for information security in their organisation.

Exposure to Digital Security Threats and Attacks

CSOs in West Africa are on the frontlines of defending democracy and human rights, but their noble efforts make them a prime target for digital attacks. With cyber criminals becoming increasingly sophisticated, CSOs are struggling to keep up with the latest security measures. Previous research (Crete-Nishihata et al. 2018; Hulcoop et al. 2016; Crete-Nishihata et al. 2014) has shown that the number of digital attacks on CSOs has increased dramatically in recent years, exposing their weak technological infrastructure to the dangers of a rapidly evolving digital landscape. For example, according to the Allianz Global Corporate and Specialty Cyber Report (2022), the frequency of ransomware attacks globally increased by about 100% from 2020 to 2021. The previous chapter of this report has also shown the high rate of digital security attacks and the most common ones that CSOs in West Africa are experiencing.

Despite the vital role they play in society, CSOs in West Africa face a variety of digital security threats on a daily basis. These dangers range from hacking and scams to the confiscation of digital devices, putting organisations, their missions, and employees at risk. It is a constant battle for these human rights and democracy advocates, who must be ever vigilant in their efforts to protect themselves against malicious actors. The digital landscape is a treacherous one, but these organisations are often determined to carry out their missions and bring about positive change in their communities. Nevertheless, in order to ensure that they can work with peace of mind, it is imperative for them to have the needed resources and support to defend themselves against digital attacks. These include access to cutting-edge technology, training and education on the latest security measures, and a legal framework that supports and protects their digital rights. With the right tools and support, CSOs can continue to make a positive impact in the world, and help bring about a more just and equal society for all.

Apart from physical resources, the importance of digital security laws and regulations cannot be overstated. Despite this, many African states still lag when it comes to enacting robust laws to protect their citizens against digital attacks (Adomako et al., 2018). Unfortunately, this lack of regulation has left CSOs in West Africa particularly vulnerable, as they are often the targets of malicious actors looking to exploit weaknesses in their technological infrastructure. The situation is further compounded by the fact that there is no widely accepted approach to regulation and response to digital security threats across the globe. This affects CSOs as they struggle to protect themselves and their data from a range of digital security threats.

Regardless of the challenges posed by digital security threats, the use of Information and Communication Technologies (ICTs) has become a vital tool for CSOs in West Africa. The widespread use of ICTs has helped CSOs to reach wider audiences and expand their advocacy efforts, making them a crucial component of their daily operations. From email correspondences, and social media to database management, ICTs have proven to be an indispensable resource for CSOs in West Africa. However, this increased dependence on ICTs comes at a cost. As the number of digital security threats continues to rise, CSOs are increasingly at risk of having their information and assets compromised.

Digital Technologies Adopted by CSOs

The cornerstone digital technologies used by the sampled CSOs in West Africa in navigating the digital realm are revealed by the data in Figure 20. The survey uncovered a universal reliance on ICTs in their daily operations.

Emails reign supreme with a staggering 99% of respondents confirming their utilisation, followed by laptops or desktop computers at 97% and mobile phones or tablets at 89%. This widespread adoption of ICTs is no surprise, as they have become the lifeblood of communication between CSOs, donors, partners, and other key players in their respective fields.

However, with this heavy dependence on technology comes a heightened risk of digital security threats like email attacks, spams, malware, and viruses. Therefore, there is the need for these CSOs to be aware of the potential dangers and to implement robust security measures to counteract them.

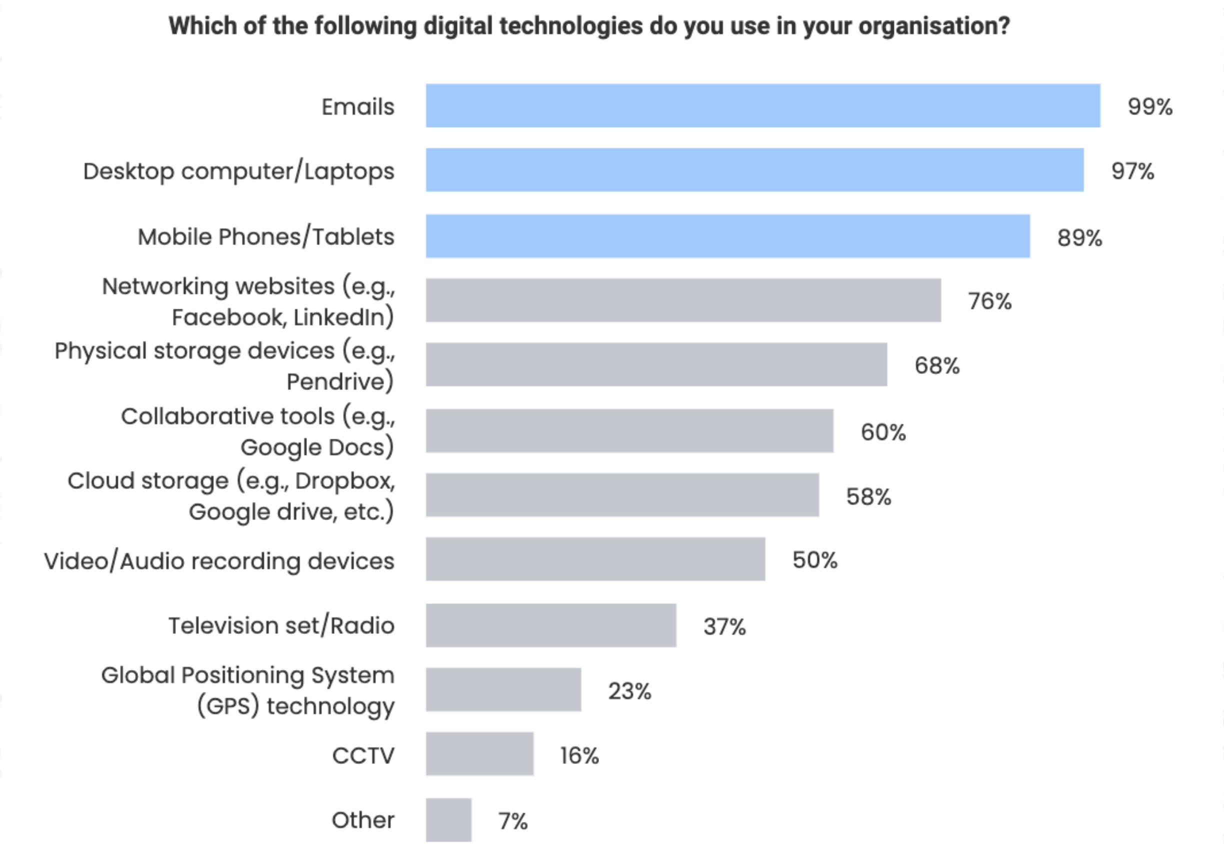


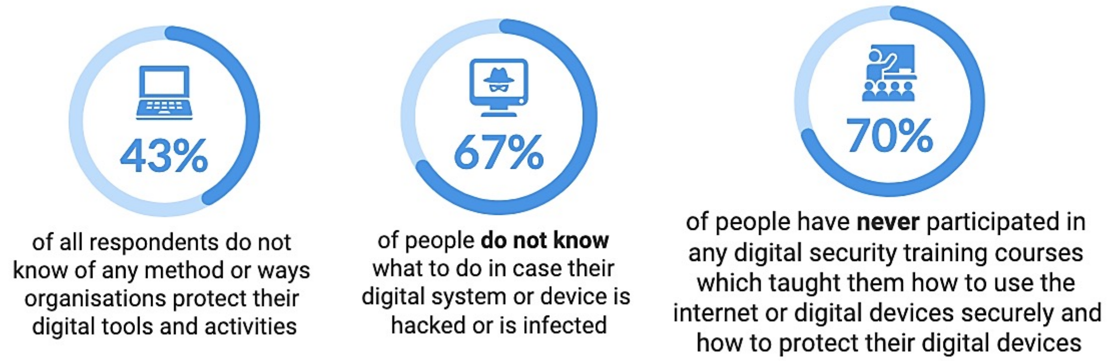
Figure 20: Digital Technologies Adopted by CSOs / Source: WACSI (2023)

Key Activities of Digital Safety among CSOs

As technology advances, the digital world becomes both a blessing and a curse. On one hand, digital tools offer unparalleled convenience and accessibility, but on the other, they also raise concerns about their security. Are CSOs aware of any methods to fend off cyber-attacks? Do they know who to contact in case their digital device or system is attacked? Are they adequately trained in protecting their digital devices? Figure 21 sheds light on these critical questions about CSOs safeguarding digital assets and maintaining their integrity in the virtual world.

The survey results reveal a concerning disconnect between the widespread use of ICTs by West African CSOs and their knowledge of digital security practices. A stunning 43% of respondents were unaware of the methods used by organisations to protect digital tools, and 67% were unsure of what to do in case of a hack or infection.

The situation is compounded by a low level of digital security skills among CSOs, with 70% of respondents reporting they had not undergone any digital security training. This raises the question of whether these organisations are equipped to handle potential digital threats and protect their digital operations.



43%

of all respondents do not know of any method or ways organisations protect their digital tools and activities

67%

of people **do not know** what to do in case their digital system or device is hacked or is infected

70%

of people have **never** participated in any digital security training courses which taught them how to use the internet or digital devices securely and how to protect their digital devices

Figure 21: Key Activities of Digital Safety among CSOs / Source: WACSI (2023)

This lack of digital security awareness and understanding among CSOs in West Africa is alarming, as the high use of ICTs in their operations makes them vulnerable to digital threats such as cyber-attacks, data breaches, and hacking. This partly explains the high rate of digital threats and attacks recorded in Chapter two. The lack of digital security skills leads to the mismanagement of ICTs, inability to implement the necessary measures to secure digital devices and systems, or detect and respond to potential threats effectively. Consequently, this results in compromise of their digital assets and their operations, leading to the loss of critical information and resources.

Secure Digital Practices among CSOs

The results from the study delve deeper into the digital security habits of CSOs in West Africa. It appears that these organisations take their passwords seriously, with a whopping 95% of respondents indicating the use of strong passwords. Unfortunately, this is where most of their digital security practices end. Despite being a crucial aspect of digital security, a concerning 68% of respondents admitted to not using firewalls or network filters to protect their devices. Similarly, only 51% of respondents reported updating their operating system with the latest security patches. The lack of digital security skills becomes even more apparent with 37% of respondents not using encryption to protect their emails and digital data and a mere 20% relying on virtual private networks (VPNs).

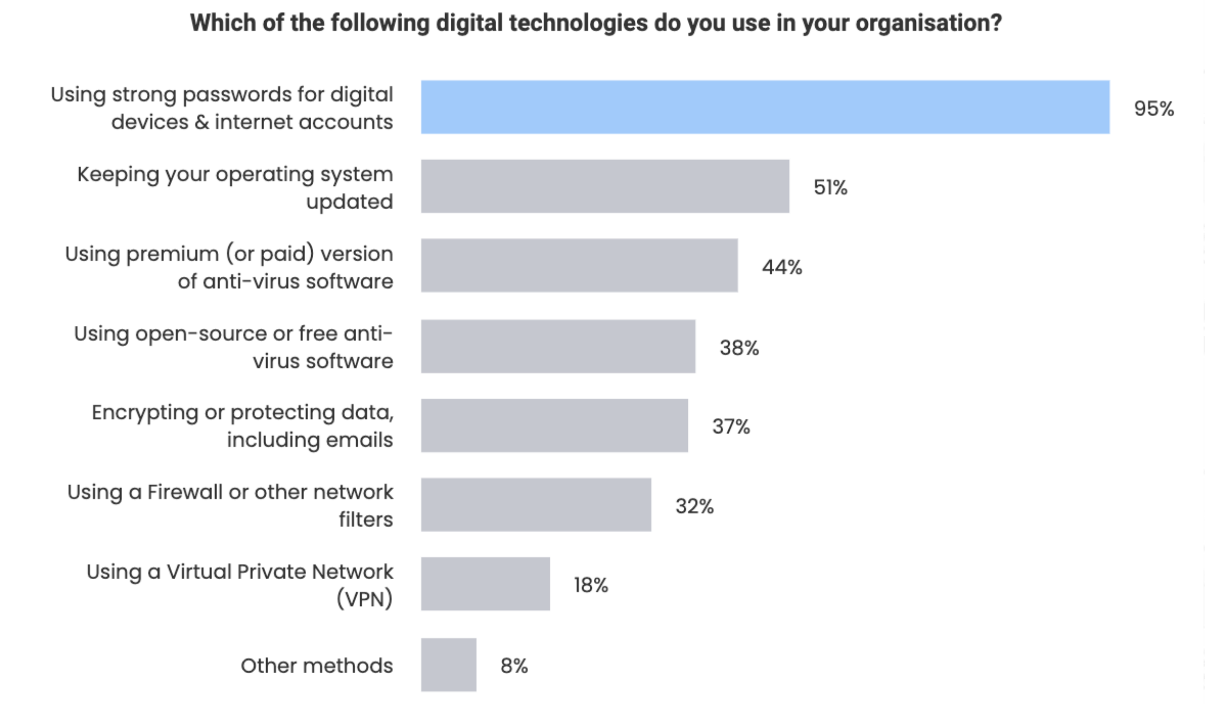


Figure 22: Other Digital Technologies Adopted by CSOs / Source: WACSI (2023)

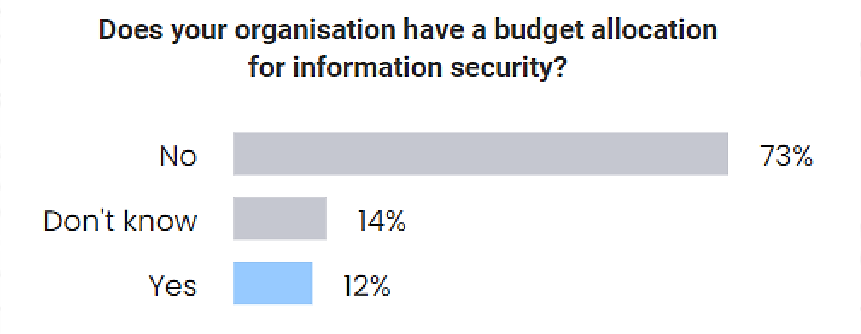
What do these statistics imply? Firstly, despite the potential widespread use of strong passwords, the results show that other critical digital security practices are severely lacking among CSOs in West Africa.

More than two-thirds of the respondents did not have any network filters or firewalls in place to protect their devices, which is a crucial step in safeguarding digital information. Likewise, it is alarming that less than half of the respondents reported keeping their operating systems up to date with the latest security patches. This puts their digital devices and systems at a higher risk of being hacked or infected by malware.

Moreover, 37% of the respondents did not use any encryption methods to protect their digital data and emails. This means that if their devices were hacked, their information could easily be stolen, leaked or misused. In the current digital age, encryption has become an essential security measure to protect sensitive information. Also, with only 20% of the respondents reporting using VPNs to encrypt their internet traffic, the majority (80%) are left vulnerable to attacks when connected to public networks particularly outside the organisation. These results indicate that there is a need for CSOs in West Africa to upskill and equip themselves with the knowledge and tools to protect their digital devices and data.

Digital Security Budgetary Allocation among CSOs

Protecting digital safety is a costly venture, but essential for the success of CSOs. As highlighted by Henrichsen et al. (2015), the irregular funding schemes of these organisations make it difficult for them to sustain robust digital security systems. To shed light on this challenge, the survey delved into the budget allocation for information security among CSOs in West Africa, the results of which are depicted in Figure 23.


Does your organisation have a budget allocation for information security?

The findings from the survey paint a bleak picture for digital security preparedness among CSOs in West Africa. With a whopping 70% of these organisations lacking the financial capacity to allocate a budget for information security, their ability to protect their digital tools and systems is severely limited. The result is a disturbingly high vulnerability to digital attacks, with these organisations unable to secure their devices with essential technologies like antivirus software or respond effectively to any security breaches that may occur. This lack of financial resources highlights the need for more support and investment in digital security for these organisations.

The limited financial resources of CSOs in West Africa are also an obstacle to hiring knowledgeable IT personnel capable of managing and securing their digital systems. As a result, these organisations are unable to implement robust digital security measures, leaving them vulnerable to various types of digital attacks that compromise the sensitive information they handle and the critical missions they undertake. This presents a challenging task for CSOs to ensure the security of their digital operations, as setting up a robust digital infrastructure demands a significant financial investment that many of them simply cannot afford. The importance of digital technologies and the financial limitations for securing digital infrastructure are highlighted by a respondent (KII15) in Box 3.1, which points to the potential risks of data breaches, financial losses, and harm to the reputation of CSOs that lack the necessary resources to secure their digital assets.

Box 3. 1: Connected but Vulnerable / Source of excerpt: KII15

CASE STUDY

The case highlights the increased use of Information and Communication Technologies (ICTs) among CSOs in Nigeria due to the COVID-19 pandemic. The pandemic led to the need for CSOs to transition from physical to virtual activities, including meetings, trainings, and community actions. The transition was a challenge for the CSO mentioned in the excerpt as they only had limited technology resources and infrastructure, such as one desktop computer and two laptops. The organisation received support from another organisation, WASCI, in the form of laptops, which improved their ability to work remotely.

Our organisation is a non-profit organisation working in the areas of environment and social justice. The COVID-19 pandemic made us realize the importance of technology in our interventions. Prior to that, our activities were mostly physical. We would go to meetings, organize community actions, mobilize community members, etc. Nobody ever thought there would be a time when activities would become virtual, but that's what COVID-19 brought.

At the initial stage, it was a big challenge to navigate through the process because we had only one desktop computer and two other laptops. Even communicating was a challenge because at that period, there were restrictions on movements, so we couldn't communicate effectively except using our phones. There were certain jobs we couldn't do, and we were limited. However, during one of our discussions during that COVID-19 period, I requested for laptops from WASCI, and they were able to facilitate my organisation. We received three laptops, and that really assisted our work through Teams and through other networks. In-person meetings now became limited, and with the help of other apps, we could work online, share correspondence, schedule meetings, run online training sessions, and have online meetings. However, we faced some challenges, such as poor internet connectivity, high data costs, which we never budgeted for, and cyber security issues. During one of our Zoom meetings, the meeting was hacked halfway, and it was very frustrating.

However, the increased use of ICTs also revealed the challenges of poor internet connectivity, high data costs, and cyber-security risks. The organisation experienced a hacking incident during a zoom meeting, highlighting the importance of cyber security in the digital age. This case demonstrates the need for CSOs in West Africa to invest in technology infrastructure, including laptops and high-speed internet, and to train their staff on safe and secure use of technology. The case also shows the need for CSOs to budget for technology and internet expenses, as well as to be aware of the potential cyber security risks and to implement measures to prevent and respond to such incidents.

The discussions with the respondent further revealed that in addition to their virtual meeting being hacked halfway, the CSO also suffered multiple attacks including hacking of their Facebook account and a virus attack via an email attachment, which resulted in data losses. In consequence, they had to seek the services of an external person which further complicated issues for them.

CSOs' Concerns about Operating Online

Different CSOs have different digital security concerns. The main drivers of this include the type of job an individual performs within a CSO and the inadequate level of awareness of the existence and dangers of online attacks (Henrichsen et al., 2015). To this end, the survey examined the main concerns in operating online, as shown in Figure 24.

The survey results suggest that CSOs in West Africa are more and more concerned about the safety of their information. Given the increasing use of ICTs and online activities among CSOs, they regularly generate and store sensitive information about donors, partners, recipients of interventions, and other stakeholders. As a result, the ability to secure this information is crucial for the operations of these organisations as cybercriminals are constantly on the lookout for vulnerabilities to exploit.

The survey asked respondents about what they are most worried about in their organisations, and the majority of respondents (85%) responded that they are most concerned about the safety of their information (see Figure 24). This is not surprising given the sensitive nature of the information that CSOs handle, and the potential consequences of a data breach or cyber-attack, such as loss of funding, reputational damage, and legal liabilities.

The high level of concern about the safety of information among CSOs in West Africa has significant implications for their digital security. It highlights the need for these organisations to invest in robust information security measures to protect their sensitive data, as noted severally in this report. This includes implementing data encryption, access controls, and regular security audits, as well as training employees on safe information handling practices. Additionally, it also means that the CSOs should consider registering with a data protection agency.

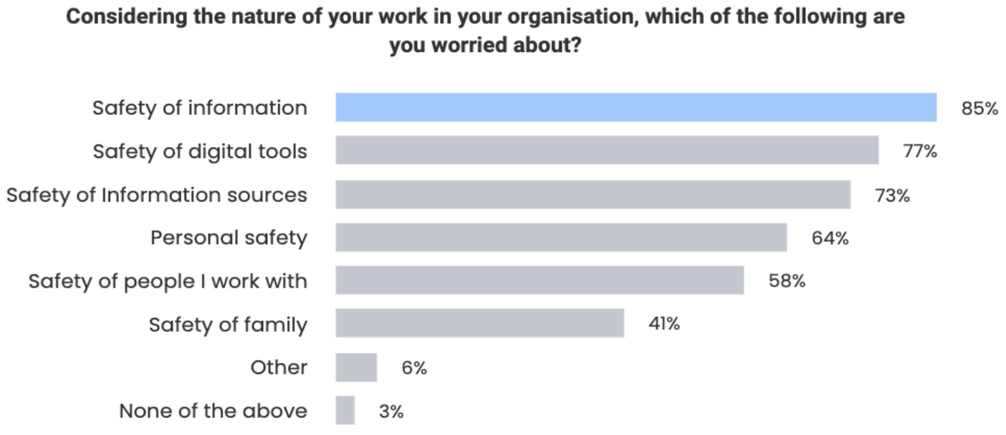


Figure 24: CSOs' Concerns in Operating Online / Source: WACSI (2023)

The social and financial costs of digital attacks

Digital security attacks can have severe social costs for the affected CSOs. Many of the CSOs that have experienced these threats lost the trust and reputation among their clients, donors, and other stakeholders, as reported in Chapter two and most of the case studies (e.g., by KII3, KII4, and KII19). For instance, KII3 lost a donor[1], along with the accompanying financial support, which had a significant impact on the organisation's ability to continue its operations (see Box 2.5 in Appendix 2).

Moreover, some of the CSOs experienced disruptions in their operations, including system downtime, data loss, and inability to access critical information. Some lost a significant amount of time trying to repair the damages caused. The attacks caused delays and, in some cases, the cancellation of planned activities (e.g., KII15). Others suffered a negative psychological impact from the attacks. All these devastatingly affected the activities of the CSOs. Beyond social costs, digital security attacks can have significant financial implications for CSOs in West Africa. The cost of an attack can for example, go beyond the replacement of stolen ICT devices, as seen in Table A3 (in Appendix 1), which estimates the cost of replacing stolen devices such as desktops, laptops, tablets, mobile devices, storage devices, and network devices.

The estimated costs for CSOs based on reported incidents in Nigeria and Ghana are $10,658.66 and $6,115.76, respectively (covering 5 desktop computers, 15 laptops, 4 tablets, 5 mobile phones, 4 storage devices, and a network device in the case of Nigeria; and a desktop computer, 11 laptops, 8 mobile phones, 2 storage and network devices, in the case of Ghana.

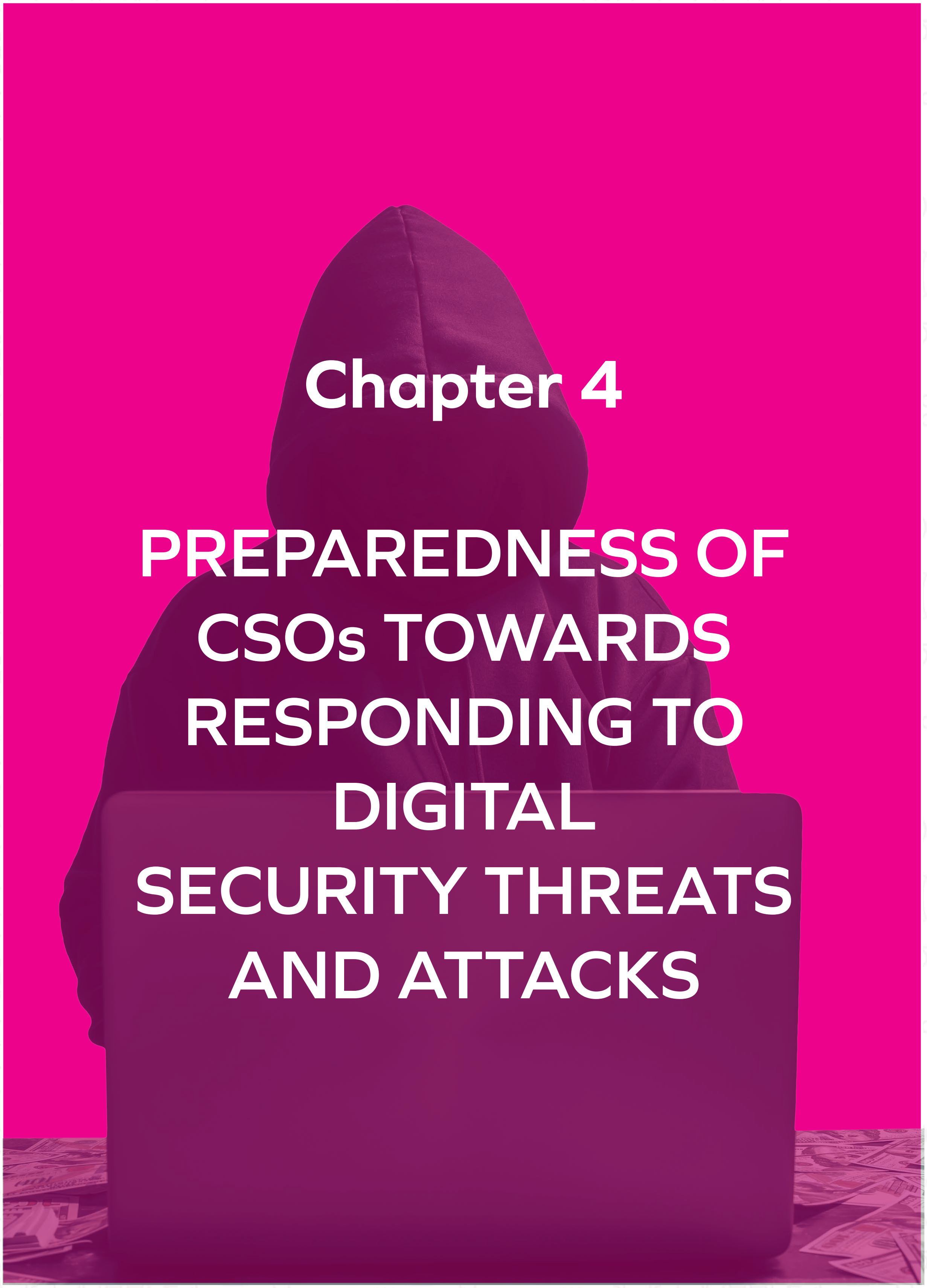
It is essential to note that the above estimates are only a part of the overall financial cost of a digital security attack. The total cost of a data breach, including lost data, incident investigation, regulatory fines, penalties, client notification, crisis management, and class-action lawsuits, can be significantly higher, as shown in Table A4 (also in Appendix 1).

The estimated total cost of data breaches for a CSO in West Africa is an average of $592,442[2], which can severely strain the finances of small and medium-sized organisations.

Therefore, investing in a robust digital security infrastructure and putting in place preventive measures to secure data might be more cost-effective than bearing the costs of an attack. These costs can put a strain on the organisation's budget and divert resources from their core missions.

[1] This happened after the CSO's Facebook account was hacked and used to solicit for funds by the attackers.

[2] This estimate includes data loss ranging from 1000 to 4000 records, incident investigation, client notification or crisis management, regulatory fines & penalties, personal card information (PCI) and class action lawsuit (see Appendix 1).



Chapter 4

PREPAREDNESS OF CSOs TOWARDS RESPONDING TO DIGITAL SECURITY THREATS AND ATTACKS

This chapter focuses on the level of preparedness of CSOs in responding to digital security threats and attacks. It examines the preparedness of CSOs in West Africa in responding to digital security threats and attacks, and the relationship between low digital security awareness and skills, and experiences of threats and attacks.

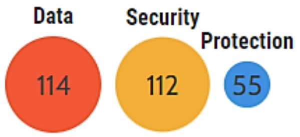
Key Insights

39%

of respondents who have some knowledge or skills in digital security **taught themselves** how to secure their digital devices and activities online.

92%

of respondents have received guidance on **using strong passwords** and two-factor authentication for Internet accounts. Sadly, this is where digital security preparedness end for most.



114 mentions of "**data**" and "**security**" (112 mentions). Data security and protection were therefore the most commonly cited topics on which respondents would be interested in receiving training

CSOs' Readiness to Tackle Digital Threats

Civil Society Organisations (CSOs) in West Africa are facing a plethora of digital security threats as shown in the previous chapters. These threats include cyber espionage, malware, phishing, ransomware, among others which can compromise the confidentiality, integrity, and effectiveness of their operations.

Many CSOs in West Africa are particularly vulnerable to digital security threats due to a number of factors, including limited ICT infrastructure, limited partnerships and collaborations, limited understanding of digital security risks, limited engagement with stakeholders, and inadequate budget.

Each of these factors can contribute to the exposure of CSOs to digital security threats, making it more difficult for them to protect themselves and continue their important work in the region. In this context, respondent KII8 underscores the usefulness of social media for instance, whilst acknowledging CSOs' vulnerabilities in employing the social media tool (see Box 4.1).

Box 4. 1: The Value of Social Media to CSOs / Source of excerpt: KII12

CASE STUDY

To some CSOs a presence on social media means more. In the excerpt, a key informant from a CSO in Nigeria discusses the importance of social media, and hence digital security for their organisation. The CSO works on themes such as governance, enterprise development, and sexual reproductive health and rights. They mention that they use social media extensively as a means of reaching their target group of young people, and that they employ various tools to prevent cyber-attacks, such as two-step verification. However, they mention that they have experienced a hack attempt on one of their social media. The informant adds that if the attempt had been successful, it would have led to a big loss, more than just a social media account.

We have a lot of information on this social media platform from the very beginning of our organisation, so it tells the history of our organisation, and we have lost some of it already as we had our hard drive crash at some point in time. We have had two hard drives crash, so we sometimes fall back on what we have already posted online to retrieve these pictures back. If we lose our social media account, we know we have lost virtually everything we know about the history of the organisation. When a potential funder wants to check our history, that is where they go to see if we are really doing work on Sexual Reproductive Health and Rights, governance, or whatever. If we don't have that, it's like starting all over again, and we can't go back to those times to bring those moments back. So, for me as a media person, I can't afford to lose anything we have on social media. If I can lose what I have on the hard drive, I can't afford to lose what I have on social media. It's quite severe in my mind.

Had the attempt been successful, the organisation would have been at risk of losing sensitive information, such as their history and past work, which is stored on their social media accounts. They also mention that if their account were to be hacked, it would be difficult to restore trust with stakeholders, including potential funders, who rely on the organisation's social media presence to verify their legitimacy. Additionally, the informant highlights the value of social media to the organisation, noting that it serves as a historical record of their work and that losing access to this information would be detrimental. They also mention that a loss of their social media account would be severe, as it would be difficult to regain the lost information and trust with stakeholders. Generally, it can be inferred that other CSOs in the region can learn from this experience to be more vigilant and proactive in securing their social media accounts and digital information. It is important to have strong passwords, two-factor authentication and to be aware of phishing attempts and other forms of cyber-attacks. It is also important for CSOs to have backup systems and regular back-ups of their digital information, to minimise the risk of data loss.

The increasing reliance of CSOs on digital platforms has been identified as a key driver of significant digital security challenges around the world. This status quo is worsened by the loopholes in the digital capacities of law enforcement agencies and staff of CSOs who are often part of the easy victims of cybercrimes (INTERPOL, 2021). These loopholes present thriving grounds for criminal networks as online attackers across regions including Africa have clearly managed to build a sophisticated digital infrastructure that exploits the identified vulnerabilities (ibid). Many countries in West Africa have limited or poor ICT infrastructure, which makes it difficult for CSOs to access reliable and secure networks, or to use the latest technologies and tools to protect themselves against cyber threats. This makes them more vulnerable to digital security attacks, such as phishing, malware, and ransomware. Empirical studies have shown that the level of preparedness of CSOs in this context has not lived up to expectations (INTERPOL, 2021). CSOs including media actors, often do not possess the financial capacity to purchase commercial software that enhances their online security (Cogburn, 2004). As a result, they resort to free, open-source online security technologies. Though this may prove cheaper, many open-source technologies do not usually offer full protection against threats. The limited budget of CSOs in West Africa makes it difficult for them to invest in cybersecurity software, hardware, and services that can help to protect against cyber-attacks.

Another obstacle CSOs in West Africa face in their efforts to tackle digital security threats is the lack of reliable information on ICT expertise sources for assistance in mitigating online threats or attacks. Despite the availability of digital security experts willing to provide support, many CSOs have limited partnerships and collaborations with other organisations that specialise in digital security. This makes them more vulnerable to digital security attacks as they lack access to the necessary support and resources to address cyber threats. Inadequate awareness of potential digital security threats or a lack of understanding of the implications of digital threats or attacks for their psychological and physical wellness also reflects the ill preparedness of CSOs to tackle digital security threats. Apart from lacking essential digital security technologies, many CSOs are not adequately skilled to encrypt or secure their information sources and other forms of communication with partners. Digital safety training programmes organised for CSOs are often not systematic, comprehensive, or practical enough to guarantee secure and safe operations within the digital space (Henrichsen et al., 2015). This makes them more vulnerable to digital security attacks, as they may not be able to identify and respond to cyber threats effectively.

The relationship between digital security awareness and threat experience

The level of digital security awareness and skills possessed by CSOs is a critical factor that influences their susceptibility to digital threats or attacks. Previous research found a negative correlation between the frequency of digital threats or attacks experienced by CSOs and their level of digital security awareness and skills. This suggests that CSOs with low levels of digital security awareness and skills are more likely to experience digital threats or attacks. According to Henrichsen et al. (2015), media actors and CSOs in general that have received comprehensive and well-structured digital security training are less likely to experience frequent digital threats or attacks.

Adomako et al. (2018) emphasised the importance of staff digital security awareness and skills in ensuring digital safety for CSOs in West Africa. However, many CSOs in the region lack awareness of the risks they face from cyber attacks and do not have the necessary knowledge or skills to protect themselves against these threats. Consequently, they may resort to poor security practices such as using weak passwords, not updating software, or not backing up data. Moreover, the lack of cybersecurity awareness and education also applies to CSO staff who may not be aware of the risks they pose to the organisation by clicking on phishing links or using unsecured networks. Many CSOs do not have the resources or expertise to develop and implement effective cybersecurity policies and procedures, which makes them more vulnerable to cyber attacks. This lack of capacity is often compounded by the absence of a clear cybersecurity framework for CSOs in West Africa. The lack of cybersecurity awareness and education, the limited resources and capacity of the CSOs, all make it difficult for them to invest in cybersecurity training and awareness programmes. It is therefore not surprising that, Adomako et al. (2018) recommend massive public awareness and training as the key highlights for maintaining adequate online safety. They charge both private and public organisations with the responsibility of raising digital security awareness and providing effective training to staff to avoid digital threats or attacks, secure their computer networks, build customer confidence, establish social responsibility, and enhance staff wellbeing. This recommendation is supported by a participant in Guinea-Bissau (KII10) who emphasised the positive influence of digital training in combating digital threats by creating awareness among CSOs, developing an organisational-level digital strategy, and providing basic steps for digital security such as password management (see Box 4.2).

Box 4. 2: From Vulnerability to Strength: The Tale of a CSO in Guinea-Bissau / Source of excerpt: KII10

CASE STUDY

The excerpt below is from a key informant interview with a CSO representative from Guinea-Bissau discussing their experience with digital security training provided by WACSI. The interview highlights the impact of the training on the CSO's digital security practices. The training emphasised the importance of strong passwords and the need to regularly update and change them. The CSO was also made aware of the dangers of clicking on suspicious links and was advised to examine the source of links before clicking on them. The CSO representative also mentioned the need for antivirus protection and the dangers of exposing sensitive information on social media platforms like Facebook and WhatsApp. The interviewee emphasised the change in behaviour that resulted from the training, with the organisation now regularly updating passwords to maintain digital security.

The training we received from WACSI was an excellent addition to our data protection. It was particularly helpful when they talked about creating strong passwords and not clicking on just any link. There are many scammers out there, so it's essential to verify the source of any links before clicking on them. We were also well-informed about antivirus software and the importance of keeping it up-to-date to protect against unhealthy information. We have also learned about the connection between Facebook, WhatsApp and our data, and we take measures to avoid being over-exposed. We try to change our passwords and upgrade our security at the end of each month. This has become a habit that has greatly improved our digital security.

The experience of the CSO highlights the importance of digital security training and awareness for CSOs in West Africa. The increasing use of Information and Communication Technologies (ICTs) among CSOs in the region has led to an increased risk of digital attacks and cybercrime. Thus, providing digital security training and creating awareness among CSOs is crucial to mitigate these risks and ensure the protection of sensitive information. This experience also highlights the need for robust digital infrastructure and the need to regularly update and maintain it to prevent security breaches.

Interestingly, when asked whether their organisation has experienced any digital security threats or attacks in the last 12 months, the respondent answered: *There are links that we often receive but we do not know the source...we often delete them because we do not know the origin and that's what encourages us to improve our password.*

This excerpt highlights the awareness and caution taken by the organisation towards potential digital security threats, such as suspicious links. The respondent mentions that the organisation often receives links of unknown origin, which prompts them to take measures to improve their password security. This shows that the organisation is taking proactive measures to protect itself from potential digital security attacks and breaches. The practice of deleting unknown links is a good habit that helps minimise the risk of falling victim to phishing scams or malware infections. However, simply improving passwords may not always be sufficient to fully protect against all types of digital attacks, and other security measures such as anti-virus software and network security should also be considered. Overall, this response demonstrates the importance of digital security awareness and the need for organisations to adopt comprehensive security measures to protect their data and information.

The respondent was further asked whether their organisation has a digital security policy. The respondent answered: *Now, I can't say yes or no about our security measures because the training we received from WACSI is what we are using to improve our digital security. We don't have a specific policy yet, that's why we've asked WACSI to provide us with software that can help us implement their recommendations. Overall, we are relying on the recommendations given by WACSI to guide us at this time.*

The respondent mentions that their organisation received training from WACSI on digital security, which they are trying to incorporate into their security measures. However, they do not currently have a specialised digital security policy in place. Instead, they are relying on the recommendations made by WACSI as a guide. The respondent also mentions that they are seeking assistance from WACSI in implementing a digital security policy by providing software. This suggests that the organisation is aware of the importance of digital security but lacks the necessary resources or expertise to fully address these concerns. The lack of a formal digital security policy also increases the organisation's vulnerability to digital security threats and attacks. Therefore, it would be beneficial for the organisation to establish a digital security policy and obtain the necessary resources and support to implement it effectively. The key informant added how a digital security policy could benefit their organisation.

Having a digital security policy within our organisation will help to reduce many more threats, if not end them completely. We can all apply the training we received from WACSI online, and share reminders to help us safeguard our data. Before, when we were searching for funding, we clicked on any link that came our way, even if they were fake. Now, since we've received the training, we know better than to click on just any link, and we regularly review our passwords.

The respondent recognises the importance of having a digital security policy within the organisation. The respondent suggests that such a policy could help reduce digital security threats and provide guidelines for the safe handling of sensitive information and data. They mention that the training received from WACSI has already helped them to improve their data protection practices, such as avoiding clicking on links from unknown sources and regularly reviewing passwords. The respondent also highlights that the training has helped raise awareness among the organisation's members about the importance of digital security and has changed their behaviour regarding online security practices. This highlights the positive impact that digital security training and awareness can have on organisations in West Africa. The respondent suggests that having a specialised policy in place could reinforce these practices and further reduce the risk of digital security threats and attacks.

It is however interesting to note that, despite the efforts of some CSOs to prevent cyber-attacks, the measures they sometimes implement are not adequate to protect them from threats. This is why there is no such thing as being over protected when it comes to digital security. As demonstrated in Box 4.3, even with various security measures in place, a CSO (KII12) still experienced attempted hacks and suspicious emails. This case study highlights the need for CSOs in West Africa to remain vigilant and take proactive measures to ensure their digital security.

Box 4. 3: No Such Thing as Being Over Protected / Source of excerpt: KII12

CASE STUDY

This case describes a situation where a civil society organisation (CSO) that experienced digital security challenges. The CSO works with young people and focuses on three thematic areas: governance and policy, enterprise development, and vulnerability and Sexual Reproductive Health and Rights. They use various social media platforms to reach their target group and have implemented various security measures such as two-step verification to prevent cyber-attacks. However, despite these efforts, the CSO has recently experienced an attempted hack on their Instagram account.

Recently, I noticed that somebody from another state in Nigeria tried to hack into our Instagram account. Whenever we receive notifications that someone is trying to log into our account, I check with my colleagues who have access to our accounts to confirm if they are the ones. I change our password if necessary. On another occasion, we received an email to our organisation's email address, saying we should click on a link. It was a fraudulent message, so I knew it was a security threat. They usually hack into your accounts and start sending messages to your stakeholders, asking for money or to donate to a particular cause. We don't ask for money that way. We have noticed that a few pages on our website have gone missing, such as our staff profile and board of trustees' pages. I'm not sure if this is an internal or an external threat. I don't know how to handle it.

Additionally, the CSO received a suspicious email on their organisation's email address that they believed could have been a fraudulent message. The informant also mentioned that several pages on their organisation's website went missing, and they were unsure if it was due to a security threat or an internal issue. These experiences indicate that the CSO may not be completely protected from digital security threats despite their efforts to prevent them. The organisation may have to further review their security measures and be more vigilant in monitoring for suspicious activity to minimize the risk of a successful attack. CSOs in West Africa can learn from this experience by understanding the importance of implementing security measures such as two-step verification, being vigilant about suspicious messages and emails, and regularly monitoring their website and social media accounts for any unusual activity. They can also consider hiring experts to help with their website's back-end to ensure that their websites are secure. They should be familiar with the common types of cyber-attacks and be aware of the best practices for preventing them. Hence, the need for more training on digital security in the region. Another key take-away from this case is that, there is no such thing as being over protected when it comes to digital security. CSOs in West Africa already implementing digital security measures should be vigilant in monitoring for suspicious activity to minimize the risk of a successful attack. Additionally, they should be prepared to take swift action if they suspect an attack is taking place.

Digital security training among CSOs

This study has shown in the previous chapters that CSOs in the West African region are experiencing a significant number of digital security threats and attacks such as virus attacks, social media attacks, email attacks, and even physical attacks. All these underscore the importance of digital security training for CSOs in the region. Without proper training, CSOs may not have the knowledge and skills needed to protect themselves and their organisations from these types of threats. As the percentage of digital security threats and attacks varies from country to country, there is the need for CSOs in the region to be aware of the specific digital security risks in their country and to take the necessary measures to protect themselves accordingly.

Therefore, the study examined whether respondents have participated in any digital security training that taught them how to protect their digital devices or operate safely in the digital space. Interestingly, only about 30% of them indicated that they have participated in a digital security training programme. We further asked these 30% to indicate the type (mode) of training they received. The results presented in figure 25 show that, the majority (62%) of the respondents that have received some form of training on digital security, had their training online. It is striking to note the high percentage of the respondents who taught themselves (39%) how to secure their digital devices and activities online. However, this could also imply that these individuals may not be receiving enough training from their employer, and they may not be fully aware of the latest threats and best practices, consequently, the need for CSOs to provide regular training and guidance to their employees to ensure they are equipped to handle current cybersecurity threats.

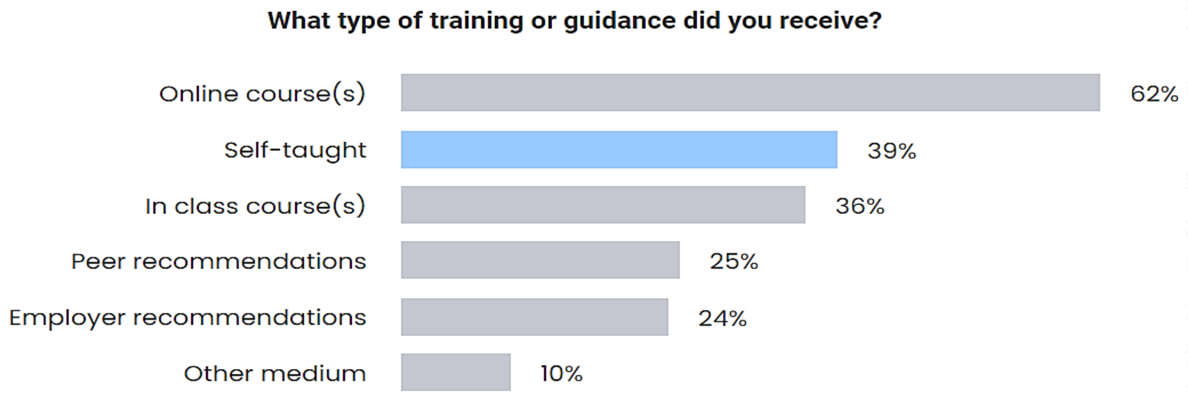


Figure 25: Training or Guidance Received by CSOs / Source: WACSI (2023)

We again asked the respondents about the exact training they received. Figure 38 shows the results. Of the 30% that received training, 92% had guidance on using strong passwords and two-factor authentication for Internet accounts. This is a positive indication that they could be taking steps to secure their online accounts and protect sensitive information. However, it is interesting to note that only a minority of the respondents received training or guidance on more advanced cybersecurity topics such as encrypting data, using a VPN, and using IP disguisers/blockers. This could imply that these respondents or CSOs may not have a comprehensive understanding of cybersecurity best practices and may be at a higher risk of a cyber-attack.

It is also worth noting that 30% of the respondents were trained or guided on using open-source anti-virus software. This Figure, together with the survey results in Chapter three (see Figure 22), which indicates that 38% of CSOs rely on open-source antivirus software for their digital security needs, have significant implications. Particularly, while open-source software can be beneficial as it is often free and can provide basic protection, it also has several limitations. This type of software is often developed by a community of volunteers who may not have the same resources or expertise as commercial software developers. This can lead to slower updates and fewer features. In addition, open-source software may not offer the same level of technical support as paid or full versions. Also, relying solely on open-source software can leave organisations vulnerable to more advanced and sophisticated attacks. Therefore, CSOs should consider investing in paid or full versions of antivirus software to ensure they have access to the latest features and security updates, as well as reliable technical support. While open-source software can be a good starting point, it should not be relied on as the sole source of protection for critical digital assets.

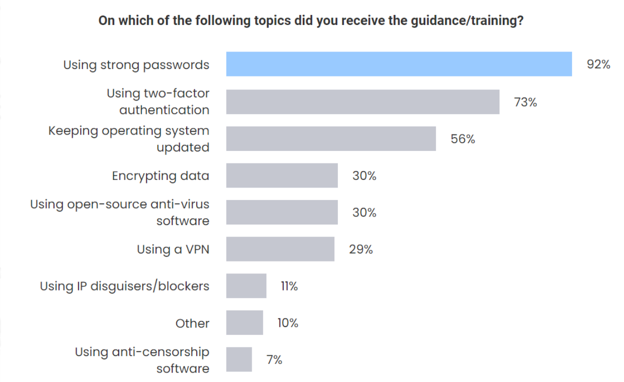


Figure 26: Topics on which CSOs have Received Training or Guidance / Source: WACSI (2023)

These statistics highlight the need to provide training and guidance on a variety of cybersecurity topics, not just the basics such as using strong passwords and two-factor authentication. Encryption and other advanced security measures can greatly enhance the security of an organisation, and CSOs should encourage their employees to take the time to learn about these topics.

During the key informant interviews, respondent KII19 shared their experience on how filling out the questionnaire for this study enlightened them to reflect on their organisation's digital security. It encouraged them to take immediate steps towards changing their passwords and activating two-step authentication for their accounts (see Box 4.4). While this is a good start, as demonstrated in the case of respondent KII12 (Box 4.3), more efforts beyond password management will be required to ensure their digital safety.

Box 4. 4: Small Acts, Big Impact / Source of excerpt: KII19

CASE STUDY

The CSO in this excerpt learned several key digital security tips from filling out the survey about digital security in West Africa. One of the main things they learned was the importance of strong passwords and regularly changing them. Prior to filling out the survey, the CSO had not been regularly changing their passwords and did not have a specific person in charge of managing their social media handles, leading to potential vulnerabilities.

After filling out the survey, as an organisation, we felt that we didn't have a specific person responsible for handling our social media accounts, and that we all had access to them. So, I reorganised and changed all the passwords after the survey. The survey made me realise that we need to change our passwords regularly, which we hadn't been doing before. So, I assigned only one officer, which is myself as the director of programs, to post all the activities. Other thematic areas can send their posts to me and I will post them. This way, they won't have access to the passwords. Since I implemented this change, nobody has tried to hack our accounts. I also change our passwords every seven days now. I learned from the survey that changing passwords regularly is very important. So, I picked up those recommendations and implemented them.

After filling out the survey, the CSO took action to re-organise their digital security practices, including changing all passwords and assigning only one officer to be responsible for posting on the organisation's social media handles. This helped to improve the security of the organisation's online presence and prevent hacking attempts. This experience highlights the importance of regularly reviewing and updating digital security practices, regularly changing passwords, creating strong and unique passwords and by assigning specific individuals to manage online presence.

The Digital Security Interests of West African CSOs

In addition to examining the digital security training that CSOs in West Africa have received, it is essential to understand what topics they are interested in learning about in pieces of trainings. This knowledge can help to identify gaps in their current knowledge and skills and guide the development of effective training programmes. Several relevant topics emerged from the study, as shown in Figure 27.

Based on the results, it appears that the CSOs in West Africa are primarily interested in learning about digital security topics such as data encryption, data protection measures, skills on how to prevent external hackers from accessing their databases, and how to establish digital security policy within their organisations. They also express a desire to learn about preventing the hacking of email accounts and how to deal with a hacked system, as well as protecting digital equipment from cyber-attacks.

Additionally, they are interested in learning about using and installing software, navigating and securing websites, and using encryption and VPNs as shown in Figure 27. The Figure (27) is a Word Co-occurrence Network diagram. It is a type of data visualisation that represents the relationships between words in a text. It is a network graph that shows how often words appear together in each corpus of text. Each node in the graph represents a word, and the edges between nodes represent the co-occurrence of words. These edges show the frequency of co-occurrences. It can be seen from the network diagram that data protection, data encryption and how to secure digital devices are of significant interest to CSOs (the biggest circles and interconnections).

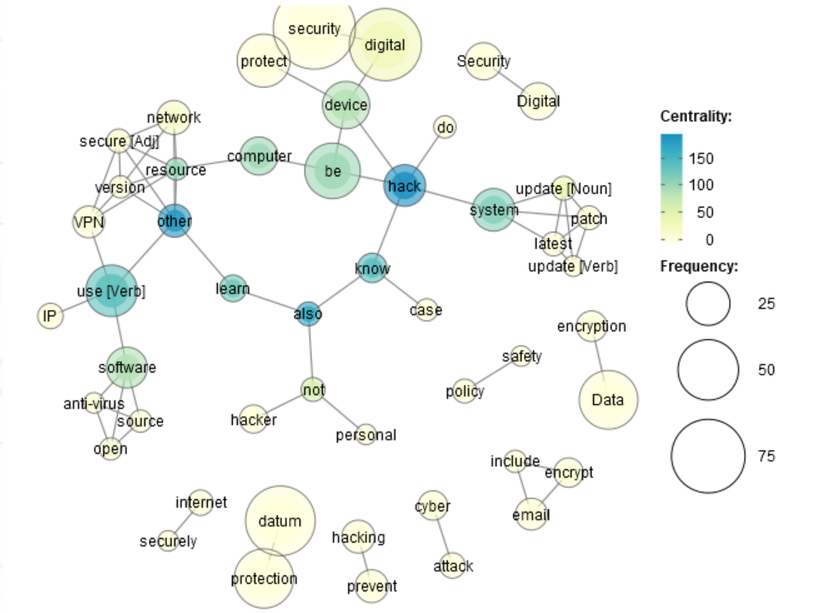


Figure 27: Topics on which CSOs are Interested in Receiving Training or Guidance / Source: WACSI (2023)

To gain further insights into the training interests of CSOs, we generated the frequency distribution of words used by the respondents in their responses and used this to generate a word cloud as shown in figure 28. The upper part of the graph shows the word cloud whereas the lower part shows the frequency of the top 10 words used by the respondents in their answers. Words like "data", "security", "system", "device" and "protection "stand out as the most used, highlighting the importance of these topics to the CSOs. This reinforces Figure 28 where the words are connected together in nodes.

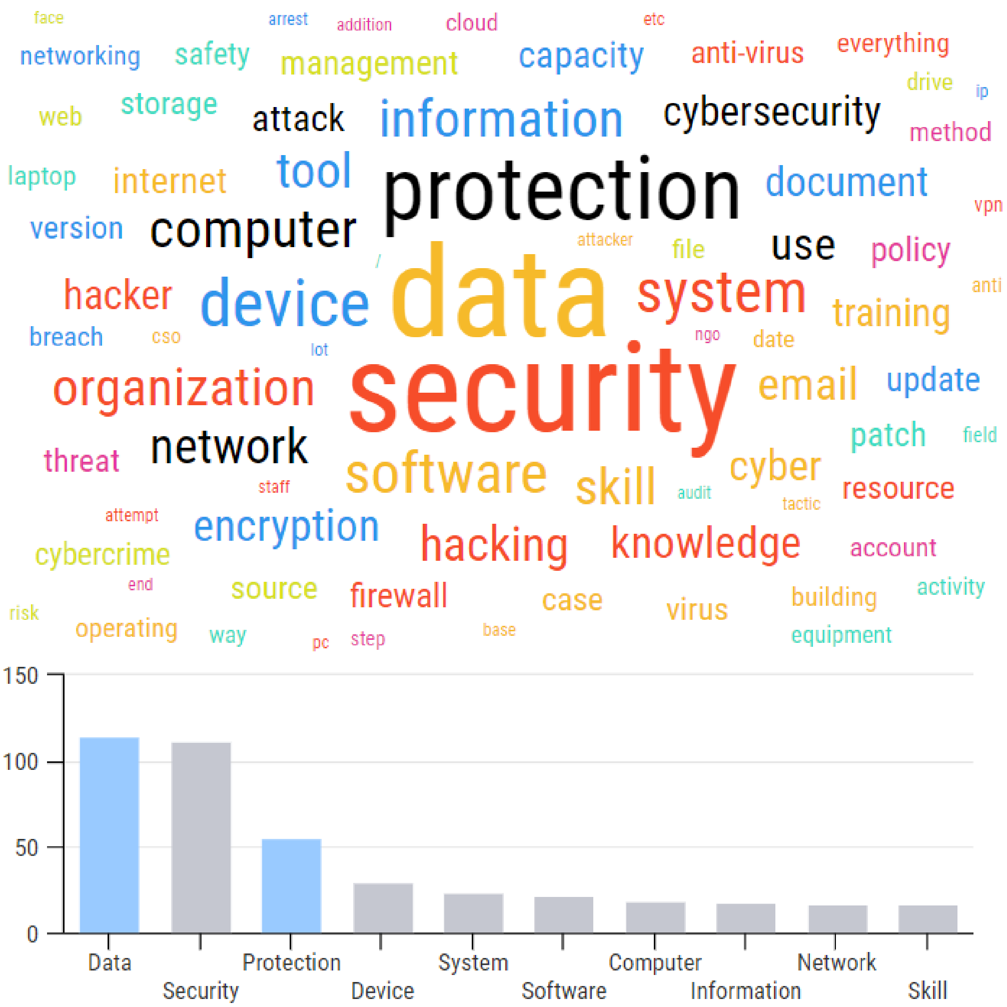


Figure 28: Frequency of Topics on which CSOs are Interested in Receiving Training or Guidance / Source: WACSI (2023)

These findings corroborate the fears expressed by the respondents regarding the safety of information in their organisation, as discussed in Chapter three. Also, these results show that there is a strong interest among CSOs in West Africa in developing their digital security skills and knowledge. It would therefore be vital to develop digital security training programmes for these CSOs, focusing on providing hands-on training and practical knowledge of the topics they have expressed interest in. This could include training on data encryption and protection measures, as well as providing skills on how to prevent external hackers from accessing their databases and establishing digital security policies within their organisations. Additionally, providing training on how to prevent emails from being hacked, how to respond to and recover from a hack, and protecting digital equipment from cyber-attacks would be beneficial.

It would also be essential to ensure that the training programmes include components such as data management, data security measures, and data protection policies, as well as network security and the use of VPNs. Additionally, providing training on digital rights and information on the latest software and tools for protecting digital devices would be beneficial.

In order to make the training as effective as possible, it would also be vital to involve experienced professionals in the field of digital security and to provide opportunities for attendees to network with other CSOs and share their experiences. Also, providing follow-up support and resources for attendees after the training would be beneficial in ensuring that they are able to apply the skills and knowledge they have gained in their daily work. Box 4. 5 provides recommendations for designing digital security training programme for West African CSOs.

Box 4. 5: Recommendations for Digital Security Training Programme

CASE STUDY

A training programme for CSOs in West Africa should focus on providing comprehensive training on a wide range of topics related to digital security, including cyber security, digital skills and digital communication, data protection, and information management. The programme should also cover the latest trends and technologies in digital security, such as post-quantum encryption, new tactics in digital security, and antidotes to surveillance of digital devices. Additionally, it should include hands-on training on practical skills such as using anti-hacking software, encrypting data, and creating secure local networks. It should also cover incident handling, scripting, policies and guidelines and digital security information. The programme should be tailored to the specific needs and concerns of the CSOs and should be designed to be easily accessible and easy to understand. The programme should also provide training on how to protect personal data, digital materials and platforms, and how to secure the confidentiality, integrity and availability of computer systems and resources. It should also cover the protection of victims of Gender based violence.

A training programme for CSOs in West Africa could include the following components:

Cybersecurity: Covers the basics of cybersecurity, including topics such as how to protect equipment and data, manage information, update digital usage, and use security software. It could also cover more advanced topics such as post-quantum encryption technology, new tactics in digital security, and antidotes to surveillance of digital devices.
Digital skills: Developing the digital skills of the CSOs, including topics such as using anti-hacking software, encryption of data, and general digital security skills.
Data protection: Protecting sensitive data and digital materials, including topics such as, data protection, digital documents retrieval in case of hacking, and data security management.
Problem-solving: Developing the problem-solving skills of the CSOs, including topics such as identifying and responding to security breaches, and understanding the technical aspects of computer forensics.
Technical Aptitude: Honing the technical skills of the CSOs, including topics such as application security development, building private firewalls, and encryption.
Digital Communication: Developing the digital communication skills of the CSOs, including topics such as networking websites, email encryption, and using VPNs.
Current trends: Keeping the CSOs up to date with the latest trends and developments in the field of digital security, including topics such as new hacking techniques, the latest security patches, and updates.
Cloud Storage & CCTV: The safe usage of cloud storage and CCTV, including topics such as data encryption, IP disguising, and anti-censorship software.
Incident handling: This component would focus on effective incident handling, scripting, and learning more about policies and guidelines.
Phishing: Training on the latest phishing techniques and countermeasures.
Firewall protection: The use of firewalls and other network filters to protect digital devices.
Ethical Hacking: Teaching the CSOs how to identify and mitigate hacking attempts, and how to retrieve a hacked system.
Database protection and management: How to protect and manage databases and digital tools.
General IT training: Providing general IT training, including topics such as computer security and general digital security skills.
Workplace policies: How to policies for protecting digital devices and materials in the workplace.
Cybersecurity awareness: Providing regular training on cybersecurity awareness and how to protect against cybercrime.
Global positioning service: Understanding the use of Global positioning service and its importance in digital security.

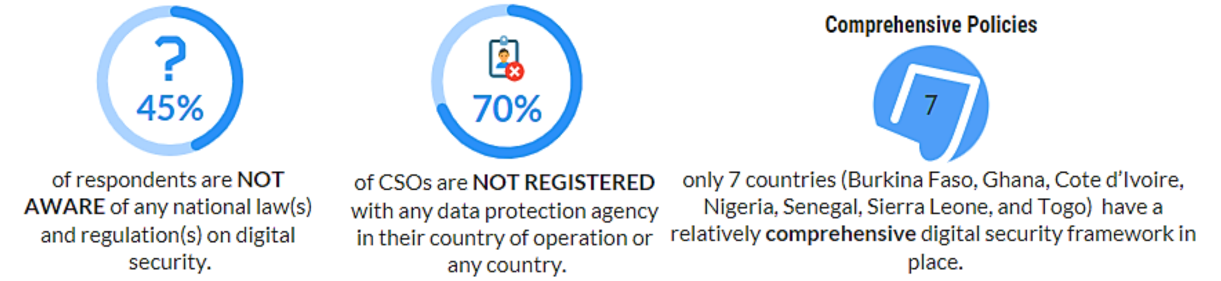
Overall, the training programme should be designed to be interactive, hands-on, and tailored to the specific needs of the CSOs in West Africa. It should also include regular assessments and evaluations to measure the effectiveness of the training and make any necessary adjustments

Chapter 5

NATIONAL LEVEL DIGITAL SECURITY LAWS AND POLICIES IN WEST AFRICA

This chapter delves into the analysis of existing national-level laws and policies regarding digital security in the West Africa region. It highlights the similarities and differences in the key provisions of the digital security regulations aimed at protecting both individuals and organisations in the region. The study examines the countries' current national laws and policies on digital security and identifies the gaps and limitations in these frameworks. It uses the African Union's (2016) requirements for digital security laws to evaluate these national policies by considering their adaptability to changing technology and criminal activity, compatibility with international laws, protection of personal data, penalties imposed, and overall comprehensiveness.

Key Insights



of respondents are NOT **AWARE** of any national law(s) and regulation(s) on digital security.

of CSOs are **NOT REGISTERED** with any data protection agency in their country of operation or any country.

only 7 countries (Burkina Faso, Ghana, Cote d'Ivoire, Nigeria, Senegal, Sierra Leone, and Togo) have a relatively **comprehensive** digital security framework in place.

Cross-country commonalities and divergences of the key contents of existing digital security regulations in West Africa

From the research, it appears that different countries have different approaches to interpreting laws related to digital security. Each country may interpret jurisdiction in accordance with their own laws. However, many countries currently lack a clear and specific digital security policy or legal framework. This means that issues such as online harassment of CSOs and theft are largely not yet addressed in their legal system. Ambiguous laws often fail to clearly define the legal liability, role, and responsibility of various online actors, such as Internet Service Providers, content providers and producers, bloggers, and CSOs, in cases of online defamation for example.

Apart from Guinea-Bissau, all the West African countries have put in place laws to safeguard the personal data of individuals. For instance, the Ghana Data Protection Act (DPA), is applicable to both data controllers and processors in various circumstances. A data controller is a person or organisation that determines the purpose and way personal data is processed, while a data processor is an entity that processes personal data on behalf of the controller (GDPR, 2016). The DPA applies in cases where data is processed in Ghana, the controller is based in Ghana, or where a controller not based in Ghana conducts business in Ghana using equipment or a data processor. This comprehensive framework for data governance, which considers the movement of data across borders, is unique among data protection regulations in Africa. Additionally, Ghana's data protection regulation imposes specific obligations on both data processors and data controllers, while in many jurisdictions, only data controllers are subject to such obligations.

The importance of protecting personal data is rooted in the fact that it is becoming easier and more cost-effective to collect and store data, including the content of emails, texts, and other communications, for extended periods. This development has made it possible to use data mining techniques, which involve searching through large amounts of computerised data to identify useful patterns or trends. For example, data mining can be used to identify potential sources of funding for civil society organisations. Meanwhile, the big data analysis market, which is often serviced by the same companies as those in consumer markets, lacks adequate oversight and checks and balances, highlighting the need for organisational data protection efforts to guarantee employee online safety and the safety of sensitive data handled by CSOs. The study investigated the extent of personal data protection among West African CSOs and found that only one-in-ten CSOs reported being registered with a data protection agency, as shown in Figure 29.

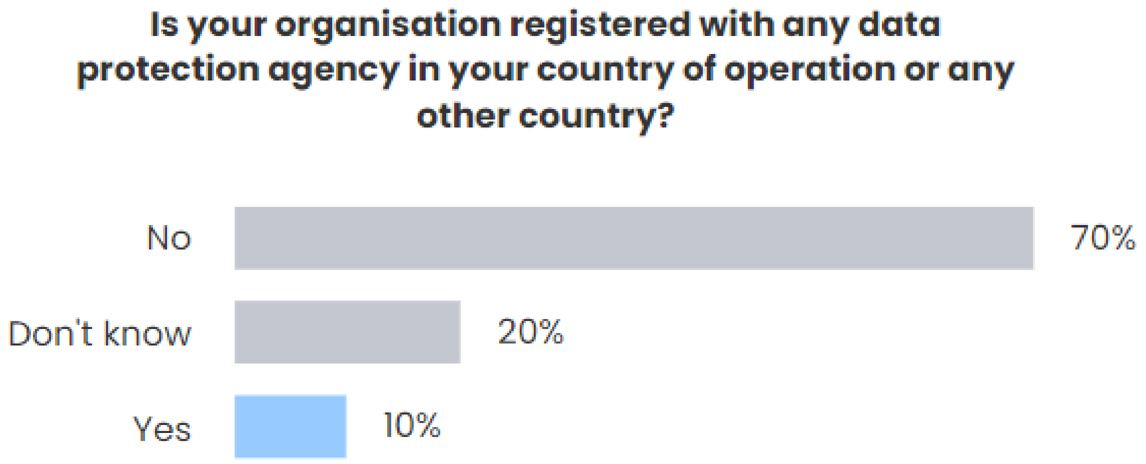


Figure 29: Registration with Data Protection Agency / Source: WACSI (2023)

With the safety of information being a major concern for CSOs, an important step that can be taken in protecting the personal data of their clients, employees, donors, and other stakeholders is to register with a data protection agency. Registration with a data protection agency demonstrates that an organisation is committed to protecting personal data and is willing to be held accountable for its actions.

By registering with a data protection agency, CSOs can also access guidance and support on best practices for data protection, such as data processing and storage policies, incident response plans, and employee training. This can help them to identify and mitigate potential risks and vulnerabilities, and to comply with data protection regulations.

The failure of CSOs in West Africa to register with a data protection agency can have significant consequences for their operations and reputation. Not registering with a data protection agency can put CSOs at risk of non-compliance with data protection laws, which can result in penalties or fines. This can also mean that CSOs miss out on guidance and support which increases the risk of data breaches and other security incidents. Moreover, reputation damage can occur if a CSO is found to be in violation of data protection laws or suffers a data breach.

This can damage the CSO's reputation among clients, donors, and other stakeholders, making it difficult for them to gain their trust (examples of such incidents have been reported in Chapter two). The loss of sensitive data can also occur as a result of data breaches or other security incidents. Finally, CSOs that fail to register with a data protection agency may be held liable for any damages arising from data breaches or other security incidents. Most of the CSOs are unaware of these potential consequences, hence, are neither taking steps to register with a data protection agency nor protect themselves against data breaches.

Meanwhile, despite Burkina Faso, Côte d'Ivoire, Ghana, Nigeria, Senegal, Sierra Leone and Togo having some fundamental legal provisions for prosecuting digital threats and attacks, there is still much to be done since there is a high level of unawareness among citizens about the existing national level digital security legal frameworks.

The results of this survey (Figure 30) indicate that there is a lack of awareness and implementation of digital security policies among CSOs in West Africa. Specifically, 45% of respondents were not aware of any national laws and regulations on digital security, 50% did not have a data backup policy or procedure, 60% did not keep logs of access to data and digital resources, 70% did not have specific requirements for password creation, and 65% did not have a documented process for creating, activating, and deactivating digital accounts.

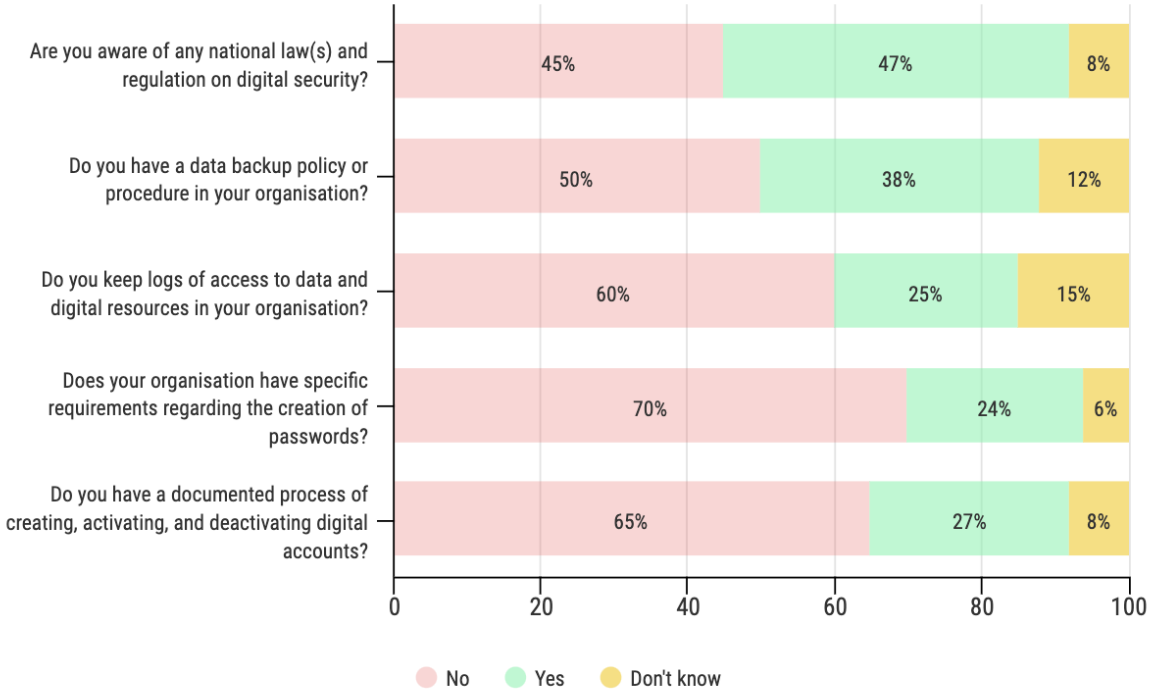


Figure 30: Level of Awareness about National Digital Security Policy / Source: WACSI (2023).

The lack of digital security policies awareness puts CSOs at risk of data breaches, and non-compliance with national laws and regulations on digital security. Respondent KII14 sums this up by revealing their CSO's email attack experience and points out that such digital attacks could be mitigated by widespread digital security awareness, due diligence when operating online, effective digital infrastructure and organisational robust digital security strategies (Box 5.1).

Box 5. 1: When Emails Attack - A CSO's Data Breach / Source of excerpt: KII24

CASE STUDY

This case describes a security breach experienced by a CSO in Liberia, where an email was received from an unknown sender that was similar to an email from their donor, USAID. The recipient, a colleague of the CSO, responded to the email without verifying its authenticity and ended up sending sensitive information to the wrong person.

An email came and the sender used an email that has not been into our system before, and then my colleague responded to the email without even consulting an executive member. The email requested for a certain report, and my colleague assumed that it was coming from USAID because we have been receiving funding from them. So, he responded without doing any detailed checks. Unfortunately, the recipient was not the intended recipient, and the information from the system was sent to the wrong person. The sender used a name similar to the donor's name, but made a slight change to the email address. For example, if the donor's name is [Odum Abukata], they would put [Odum] and maybe put [Abukati]. By the time my colleague saw the difference in the name, he had already forwarded the document. This mistake affected our system and the report that was not meant for that person has gone to the wrong person.

This experience highlights the importance of digital security awareness and the need for CSOs in West Africa to have proper protocols in place in accordance with national provision. This will help them to adopt secure practices such as verifying the identity of senders and protecting sensitive information. The use of similar names and slight changes in email addresses by the attacker shows the ease at which digital attackers can impersonate others and trick victims into revealing confidential information. The implications of this experience for CSOs in West Africa are numerous. Firstly, it highlights the need for CSOs to have a culture of security awareness and to train their staff on how to identify and respond to potential security threats, especially in their communication and information management practices. Secondly, it underscores the importance of verifying the authenticity of emails and other forms of communication, especially from unknown sources, before responding to them. Moreover, it is crucial for CSOs to have proper data management policies and procedures to secure sensitive information and ensure that such information is only accessed by authorised personnel. Finally, CSOs must also be proactive in implementing technical security measures such as secure email systems, firewalls, and encryption to protect their data and systems from potential attacks.

The convergence and divergence in the literature on the existing national level digital security laws and policies are summarised and presented in Table 3. Though the desk study of these national laws and policies does not claim to be highly extensive due to difficulties in accessing some of the laws and policies, the analysis presented here provide a snapshot-view of the regulatory environment for digital security in West Africa.

It could be thought that given the high prevalence rate of digital threats and attacks in the West African region, the countries in that region will have very comprehensive digital security laws and policies. However, contrary to this assumption, and based on criteria developed by the AU (2016) legal requirements of digital security laws, most of the national policies are partially complete, and in some instances, some of the policies and legal frameworks missed the established criteria.

The criteria rate the policies based on their dynamism with technological changes and upgrade in criminal operations, harmonisation with international digital security laws and policies, personal data protection, penalties for online crimes, and the state of the policy in terms of whether it is comprehensive or partial. After a review of the digital security regulatory framework across West Africa, we rate the countries based on these indicators and present the results in Table 3. We include an additional variable measuring how progressive or repressive the civic space in these countries is, considering that sometimes governments take deliberate actions to restrict the activities of CSOs both physically and online.

We find that many West African countries are striving to have national policies to fight digital security but, in these efforts, only half of them seem to have dynamic policies that are often updated to match the rate at which criminals change their mode of operations. Burkina Faso, Côte d'Ivoire, Ghana, Nigeria, Senegal, Sierra Leone and Togo are the countries that have developed relatively comprehensive national policies and laws to fight digital crime.

In democratic dispensations, issues of personal data privacy are paramount. This provision is reflected in the existing national digital security policies. Hence, from the review, apart from Guinea-Bissau, which virtually had no legislation on digital security, all other countries in West Africa have some form of data protection policies.

In terms of harmonisation with international digital security laws and strategies, at the global level, the Budapest Convention on Cybercrime, 2001, also known as the Council of Europe Convention on Cybercrime, seeks to address the global problem of cybercrime by establishing a common set of laws, procedures, and guidelines for countries to follow. The convention aims to improve international cooperation in the investigation and prosecution of cybercrime, as well as to enhance the protection of computer networks and systems. It also seeks to ensure that countries have effective laws and policies in place to combat cybercrime and protect the rights of individuals affected by cybercrime. As of February 28, 2023, only four West African Countries had ratified the Budapest Convention (Cape Verde, Ghana, Nigeria and Senegal)[3].

[3] See Council of Europe (2001). Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (Accessed February 28, 2023).

Table 3: Summary on Convergence and Divergence in Existing National Level Digital Security Policies

Country	Dynamism[a]	Harmonisation[b]	Protection[c]	Penalties	State of policy	Civic space[d]
Benin	I	I (E)	I	NI	P	R
Burkina Faso	I	NI	I	I	C	R
Cameroon	I	NI	I	I	P	R
Cape Verde	NI	I (B, A, E)	I	I	P	PR
Chad	I	NI	I	I	P	R
Gambia	NI	I (E)	I	I	P	R
Ghana	I	I (B, A, E)	I	I	C	PR
Guinea	NI	I (A, E)	I	I	P	R
Guinea-Bissau	NI	NI	NI	NI	-	R
Côte d'Ivoire	I	I (E)	I	I	C	R
Liberia	NI	NI	I	NI	P	R
Mali	NI	NI	I	I	P	R
Mauritania	I	NI	I	I	P	R
Niger	NI	I (A)	I	NI	P	R
Nigeria	I	I (B, E)	I	I	C	R
Senegal	NI	I (A, E)	I	I	C	R
Sierra Leone	I	NI	I	I	C	R
Togo	I	I (A)	I	I	C	R

Note: [a]Dynamic with technology and criminal operation; [b]Harmonisation with international laws; [c]Personal data protection; and [d]Civic space characterised with civic rights, laws and practices.

Key:

I = Included in the national policy on digital security;
NI = Not included in the national policy on digital security;
A = Ratified the AU Convention on Cybersecurity and data protection;
B = Ratified the Budapest Convention;
E = Alignment with the ECOWAS guidelines on cybersecurity;
C = Comprehensive national digital security framework;
P = Partial national digital security framework;
R = Repressive civic space; and
PR = Progressive civic space

Source: WACSI (2023)

At the continental level, the national digital security policies of Cape Verde, Ghana, Guinea, Niger, Senegal and Togo demonstrate a high degree of harmonisation, with the African Union's Convention on Cyber Security and Personal Data Protection 2014, also known as the Malabo Convention[4], which these countries have ratified as of February 14, 2023. The Convention aims to enhance cybersecurity and personal data protection in Africa by establishing legal and regulatory frameworks and encouraging the development of African capacity in cybersecurity, including through the establishment of national Computer Emergency Response Teams (CERTs). However, the Convention is not yet in force as it requires ratification by at least 15 members, and as of February 2023, only six West African countries have ratified it (13 in total among the 55 member countries), with six other West African countries having signed but not ratified it (Cameroon – 2021; Chad - 2015; The Gambia - 2022; Guinea-Bissau - 2015; Mauritania – 2015; and Sierra Leone – 2016).

At the regional level, ECOWAS has made significant efforts towards the harmonisation of cybersecurity laws in West Africa by developing a regional strategy on cybersecurity and cybercrime. This includes the ECOWAS Cybersecurity Strategy and Supplementary Acts on Personal Data Protection and Cybersecurity, which provide a framework for the development of national policies and laws on cybersecurity and personal data protection in the region. Although it is unclear which countries in West Africa have fully harmonised their digital security policies in accordance with ECOWAS guidelines, the policies of Benin, Cape Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Nigeria, and Senegal demonstrate a high level of alignment with ECOWAS recommendations[5].

Harmonisation with international policies presents a holistic and coordinated effort in mitigating and preventing digital crimes. However, most West African countries do not have harmonised policies that highlight the digital security laws and policy challenges in the region.

In terms of penalties, those that did not have clear sanctions for digital crimes are Benin, Guinea-Bissau, Liberia and Niger. This gap in their policies poses a threat of mis adjudication of cases and reflects partially-developed national digital security policies. Overall, the countries with the most extensive digital security policies and laws in West Africa are Burkina Faso, Côte d'Ivoire, Ghana, Nigeria, Senegal, Sierra Leone and Togo.

Meanwhile, the civic space in West Africa is generally restrictive, with only Ghana and Cape Verde having more progressive

[4] See African Union (2014). African Union Convention on Cyber Security and Personal Data Protection. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (Accessed February 28, 2023).

[5] See ECOWAS Commission (2017, September 11). ECOWAS Directive and related texts on Cyber legislation. ECOWAS-CoE Regional Conference on Cyber legislation. Retrieved from https://rm.coe.int/-3148-3-2-3-nigeria-ecowas-o-3-auc-moctar-yedaly-pdf/1680748652 (Accessed February 28, 2023) and
UNCTAD (2018, October 29). West African countries helped to harmonize cyber laws at UNCTAD workshop in Ghana. Retrieved from https://unctad.org/news/west-african-countries-helped-harmonize-cyber-laws-unctad-workshop-ghana (Accessed February 28, 2023).

environments compared to other countries in the region. This is consistent with the global trend of closing, repressing or obstructing civic space, with only 3.1% of the global population living in open environments according to CIVICUS (2022) Monitor[6] tracking the civic space of 197 countries worldwide. There have been incidents in West Africa where countries have blocked the internet or shut down social media sites and messaging apps, particularly during elections or in response to protests.

For example, the maiden deliberate network shutdown in Africa is known to have occurred in Guinea in 2007 (Rydzak, Karanja and Opiyo, 2020). Since then, many countries in the region have had similar experiences. In 2017, Cameroon introduced a three-month internet block in its Anglophone regions, and Togo shut down the internet during mass protests (CIVICUS, 2018). In 2016, Cameroon, Chad, The Gambia, and Mali shut down internet access completely before, during or after elections in response to protests (Turianskyi, 2018).

In 2018, the government of Chad imposed a ban on social media which lasted 16 months[7]. In 2019, the government of Benin shut down the internet during the country's elections[8], making it difficult for citizens to access information and express themselves online. In 2020, the government of Guinea also shut down the internet and banned protests ahead of presidential elections[9].

In short, some regulations in West Africa restrict the civic space. For instance, while having laws and regulations on personal data protection in West Africa is necessary, some regulations restrict the civic space and pose a challenge to society's freedom of expression and press. As an example, Chad has laws and protocols that protect personal data, with the Agence Nationale de Sécurité Informatique et de Certification Électronique (ANSICE) serving as the National Data Protection Authority responsible for ensuring compliance with the provisions of the Act on a national level. However, the same laws on contempt and defamation have been used to stifle government critics online and offline, which is a threat to freedom of expression and the press (Kalemera et al., 2020).

While Cape Verde's civic space appears to be relatively stable, Ghana's has been shrinking lately due to occasional physical assaults on the media (Turianskyi, 2018) and the use of "homophobia as punishment for advocacy for basic rights" (CIVICUS, 2022; 26). These incidents have significant consequences on the ability of CSOs to operate and engage with their stakeholders, emphasising the need for continued efforts to protect the digital rights of citizens and organisations in the region.

[6] CIVICUS Monitor. Quick facts. Retrieved from https://monitor.civicus.org/quick-facts/ (Accessed, 24/02/2023).

[7] See Chad Lifted the 16-Months Social Media Shutdown but Concerns Remain. https://cipesa.org/2019/10/chad-lifted-the-16-months-social-media-shutdown-but-concerns-remain/ (Accessed, 24/02/2023).

[8] See Global Internet Shutdowns. https://pulse.internetsociety.org/shutdowns (Accessed, 24/02/2023).

[9] See Internet Cut across Guinea Ahead of Elections. https://netblocks.org/reports/internet-cut-across-guinea-ahead-of-elections-xAGoQxAz (Accessed, 24/02/2023).

Some common legal provisions

One common feature of the digital security laws and policies in the West African countries is the criminalisation of cybercrime, as shown in Table 4. Many West African countries have defined cybercrime as a criminal act committed using electronic devices or networks, and prescribed punishments for offenders. For instance, Nigeria's Cybercrime (Prohibition, Prevention, etc.) Act 2015 criminalises acts of cybercrime and prescribes punishments for offenders. Similarly, Cameroon's Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercriminality, defines and criminalises acts of cybercrime.

Another key provision in the digital security laws and policies in West Africa is the protection of critical information infrastructure. Many West African countries require the protection of critical information infrastructure from cyber threats. For instance, Nigeria's National Information Technology Development Agency Act 2007, mandates the protection of critical information infrastructure from cyber threats. Similarly, Côte d'Ivoire's Law No. 2013-450 of June 19, 2013 on the protection of personal data, requires the protection of critical information infrastructure from cyber threats.

Table 4: Common Legal Provisions on Digital Security across West Africa

Legal Provision	Description	Countries	Law/Policy
Definition of cybercrime	Defines cybercrime as a criminal act committed through the use of electronic devices or networks	Cameroon, Côte d'Ivoire, Ghana, Nigeria, Togo	• Cameroon's Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercriminality • Côte d'Ivoire's Law No. 2013-450 on June 19, 2013 on the protection of personal data • Ghana's Electronic Transactions Act, 2008 (Act 772) • Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015 • Togo's Law No. 2018-026 of 071218 on cybersecurity and the fight against cybercrime
Criminalisation of cybercrime	Criminalises acts of cybercrime and prescribes punishments for offenders	Cameroon, Côte d'Ivoire, Ghana, Nigeria, Togo	• Cameroon's Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercriminality • Côte d'Ivoire's Law No. 2013-450 on June 19, 2013 on the protection of personal data • Ghana's Electronic Transactions Act, 2008 (Act 772) • Nigeria's Cybercrime (Prohibition, Prevention, Etc.) Act 2015 • Togo's Law No. 2018-026 of 071218 on cybersecurity and the fight against cybercrime

Protection of critical information infrastructure	Requires the protection of critical information infrastructure from cyber threats	Cameroon, Côte d'Ivoire, Ghana, Nigeria, Togo	• Cameroon's Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercriminality • Côte d'Ivoire's Law No. 2013-450 on June 19, 2013 on the protection of personal data • Ghana's National Cyber Security Policy and Strategy, 2016 • Nigeria's National Information Technology Development Agency Act 2007 • Togo's Law No. 2018-026 of 071218 on cybersecurity and the fight against cybercrime
Creation of national cybersecurity agencies	Establishes national cybersecurity agencies responsible for cybersecurity	Cameroon, Côte d'Ivoire, Ghana, Nigeria, Togo	• Cameroon's Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercriminality • Côte d'Ivoire's Law No. 2013-450 on June 19, 2013 on the protection of personal data • Ghana's National Cyber Security Policy and Strategy, 2016 • Nigeria's National Information Technology Development Agency Act 2007 • Togo's Law No. 2018-026 of 071218 on cybersecurity and the fight against cybercrime

Source: WACSI (2023)

Also, some West African countries have established national cybersecurity agencies responsible for cybersecurity. For example, Nigeria's National Information Technology Development Agency Act 2007, establishes the National Information Technology Development Agency (NITDA) responsible for cybersecurity. Similarly, Cameroon's Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercriminality, establishes the National Agency for Information and Communication Technologies (ANTIC) responsible for cybersecurity. Despite these commonalities in digital security laws and policies across West African countries, there are also differences in the provisions, with implications for CSOs' digital security in the region. One key difference is the existence of data protection regulations. While some West African countries have enacted comprehensive data protection regulations, others do not have such laws. Interestingly, only six (6) countries in West Africa (Benin, Burkina Faso, Cape Verde, Ghana, Mali and Senegal) have comprehensive data protection laws (Rich, 2016). CSOs in countries with comprehensive data protection laws are relatively likely to be better equipped to protect the personal data of their stakeholders and avoid data breaches. Another key difference is the resources available to national cybersecurity agencies. Some West African countries have well-funded national cybersecurity agencies with the capacity to respond to digital threats promptly. In contrast, others have underfunded national cybersecurity agencies, which are not adequately equipped to respond to digital threats promptly. This also impacts the ability of CSOs to receive timely support from national cybersecurity agencies during digital threats or attacks.

In a nutshell, the commonalities in these laws and policies indicate a shared understanding of the need to protect critical information infrastructure and criminalise cybercrime. However, disparities in provisions of digital security laws and policies also have implications for CSOs' digital security in the region. Those operating in countries with comprehensive data protection laws and well-funded national cybersecurity agencies may be better equipped to protect their digital assets and avoid digital threats or attacks.

Existing national laws and policies about digital security in West Africa

This section provides an overview of the existing national laws and policies about digital security in West Africa. Overall, Benin, Burkina Faso, Cameroon, Cape Verde, Ghana, Guinea, Côte d'Ivoire, Niger, Nigeria, Senegal, Sierra Leone, and Togo have all implemented laws, policies, or legal frameworks related to cybersecurity and/or data protection.

The Law No. 2017-20 of April 2018 in Benin provides for arrest, search, seizure, and prosecution related to digital offenses, and the Personal Data Protection Authority was established to ensure compliance with legal provisions regarding the protection of personal data.

The new Act No. 001-2021/AN of 30 March 2021, enacted on 21 April 2021, in Burkina Faso, updates and replaces the previous data protection law of 2004, establishes the Commission de l'Informatique et des Libertés (CIL) as a regulatory body, requires permission for data processing, enhances data subject rights, and increases penalties for violations.

The law/policy in Cameroon is the Cameroon Digital Strategic Plan 2020, which aims to improve internet coverage in the country through eight strategic objectives, and also includes penalties for those who violate data privacy, with employees and security audit experts of corporate bodies who disclose confidential information without permission during a security audit facing imprisonment of 3 months to 3 years and a fine of 20,000 to 100,000 CFA francs.

Law 133/V/2001, established on 22nd January, serves as the foundation for cybersecurity in Cape Verde and sets the legal guidelines for the protection of individuals in regard to the handling of personal data, with Section 9 covering topics such as suspicion of illegal activities, penalties, security measures, and violations.

The personal data protection regulations in Chad are mainly governed by Act No. 007/PR/2015 of 10 February 2015, and data collection and processing must adhere to principles and requirements, with penalties for breaches of data privacy; however, laws and regulations on contempt and defamation have been used to limit freedom of expression, with fines and the possibility of suspension for up to three months upon conviction under the press regime law of 2010.

The Information and Communication Act of 2009 in Gambia deals specifically with Computer Misuse and Cybercrime, and was amended in 2013 to criminalise online dissent, with individuals convicted of such offences facing penalties of up to 15 years in prison and/or fines of up to GMD 3 million (USD 100,000). The Cybersecurity Act of 2020 (Act 1038) establishes Ghana's Cyber Security Authority (CSA), creates a legal framework for protecting critical information infrastructures, regulates cybersecurity services, ensures the protection of children online, and develops the country's cybersecurity ecosystem. Ghana's Data Protection Act of 2012 offers a more flexible approach in defining personal data and the legal handling of data compared to the stricter standards adopted by many African countries after the implementation of GDPR. The law/policy in Guinea is Law L2010/003/CNT of 23 June 2010, which establishes a Guinean "High Authority for Communication" to ensure compliance with the principle of equality of communication users and respect for plurality, and telecommunications laws from 1992 and 2005, both of which include provisions for respect for personal data and privacy.

Guinea-Bissau lacks provisions on cybersecurity in its Basic Law (No. 5/2010) on Information and Communication Technologies and has no specific legislation addressing cybercrime, with no official national or sector-specific cybersecurity framework in place.

The Fight Against Cybercriminality Act (No 451) and The Law No. 2013-450 on The Protection of Personal Data was adopted in Côte d'Ivoire to combat cybercrime and criminal offenses that require the collection of electronic evidence, with Chapter 3 of the Act establishing penalties for committing crimes related to information systems and the internet in general, including imprisonment and fines.

There is no specific legislation addressing cybercrime issues in Liberia, however, the Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA) was established as a non-governmental agency in 2019 to provide cyber security and digital forensics education to the government and people of Liberia, and to strengthen the ability of public and private institutions to prevent and address cybercrime through policy development, training, and awareness-raising.

Mali's Law n° 2019-056 on the Suppression of Cybercrime was passed in December 2019 and aims to support reforms in the technology sector, however, several provisions pose potential risks to privacy and freedom of expression online, and there are conflicts with established rights to privacy in the Personal Data Protection Act and Telecommunications Act.

Mauritania's personal data protection is regulated by the Law No. 2017-020 of 22 July 2017, which is not yet in effect, but outlines the requirements for data processing and data subject rights, and establishes the creation of the Autorité de Protection des Données à caractère personnel (APD), which is not functional, while cybercrime in the country is governed by Law 2016-007.

Niger has enacted several laws and regulations governing data protection, cybersecurity, and cybercrime, enforced by the High Authority for the Protection of Personal Data (HAPDP), and has established the National Agency for Computer Security (ANSI) and National Authority for the Fight Against Cybercrime (ANLC) to promote awareness of digital security and combat cybercrime, respectively, while a national cybersecurity committee coordinates efforts towards a cybersecurity strategy. However, the law on the interception of digital communications has been criticised for violating the secrecy of correspondence and communications guaranteed by the Nigerien Constitution, potentially exposing citizens to persistent surveillance, and limiting freedom of expression, opinion, and the right to privacy.

Nigeria's National Security & Cybersecurity policy aims to establish a legal framework that defines the government's responsibilities in ensuring cybersecurity, and in line with this, Nigeria passed the Cybercrimes (Prohibition, Prevention, etc.) ACT, 2015, which provides a comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria.

Senegal's National Cybersecurity strategy 2022 (SNC2022) aims to create a secure and trustworthy cyberspace, and adheres to principles such as data protection laws and enforcing sanctions, with the maximum criminal punishment for security breaches being imprisonment for one to seven years, a fine of XOF 500,000 to XOF 10,000,000, or both, and an administrative punishment of up to 100 million XOF may be imposed by the Commission de Protection des Données Personnelles (CDP) as a regulatory body.

Sierra Leone's National Cyber Security and Data Protection Policy 2017-2022 aims to discourage and deter cybercriminals by strengthening the country's cybersecurity levels and collaborating with both domestic and international partners. The policy also outlines specific objectives such as increasing disruption of cybercriminals and enhancing law enforcement capabilities to combat cybercrime, with the Cybercrime Act of 2020 outlining specific offenses and their corresponding penalties.

Lastly, Togo passed a law on cybersecurity and cybercrime in 2018, followed by the Personal Data Act in 2019, and the e-ID Togo law in 2020, which established the legal framework for biometric identification data; the country has also ratified the African Union Convention on Cybersecurity and Protection of Personal Data.

All these regulations demonstrate that overall, West African countries are recognising the importance of digital security and are taking steps to address it, but there is still a long way to go to ensure comprehensive and effective protection for individuals and organisations in the region.

Gaps and weaknesses in existing digital security regulations in West Africa

The UN General Assembly conducted a study on privacy, including digital privacy, in June 2014. They found that international human rights law establishes a comprehensive and universal framework for the promotion and protection of the right to privacy, including in situations such as domestic and extraterritorial surveillance, the interception of digital communications, and the collection of personal data. However, the study also revealed that many countries have inadequate national legislation and enforcement, weak procedural safeguards, and ineffective oversight, which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy (Wafa, 2009).

Box 5.2: The Police, the Scammers, and a CSO Caught in-Between / Source of excerpt: KII17

CASE STUDY

The excerpt below is a vivid illustration of the challenges that digital security presents to CSOs in West Africa, particularly in Nigeria. The experience of the interviewee highlights how fraudsters are taking advantage of the lack of proper digital security measures and awareness to defraud CSOs and how law enforcement bodies are not providing adequate protection to citizens. The informant, who is the executive director of the NGO shared their story as follows.

I work for an NGO based in Nigeria that focuses on health and our target group is mainly women and children. Our organisation is online and anyone can find us on Facebook or our website. One day, someone claiming to be from a government agency contacted me by text message and offered a job for me and my organisation and a corresponding funding. He gave me a person's name to call and discuss how to proceed. I was initially sceptical but decided to call the number. The person answered and identified himself as Barrister Tasan from the government agency. He sounded very convincing and obtained some information from me and said that I would need to pay some money to process the payment. They requested for $2000 for processing the funding payment, which seemed suspicious. He gave me another contact person to discuss payment, and I called him too. The person also said it was real and I needed to pay some money. I became suspicious and instead of going to the bank to pay the $2000 bribe, I went to the police station to report the fraudsters. The police asked me to pay for them to apprehend the scammers. Meanwhile, the scammers kept calling me, changing the account and contact numbers. I realised they were fraudsters and did not pay them any money. They had promised to give me funding of about a billion dollars, but I discovered it was all a scam. I was following up with them to see what they would say and then eventually hand them over to the police for investigation. However, the police requested for money before they would allow me to write a statement. They asked for money to track the fraudsters, which I refused.

In the excerpt, a scammer posing as a government agency reached out to the CSO and promised funding in exchange for a bribe. The scammer even went so far as to provide multiple account numbers to receive the bribe. The interviewee, realising that this could be a potential scam, went to the police to report the incident and request assistance. However, the police demanded a bribe themselves before performing their duties. This highlights the issue of corruption and neglect of duty among some law enforcement bodies in West Africa, which sometimes leaves CSOs with nowhere to turn to for protection in times of need. The experience of the interviewee also highlights the importance of proper digital security measures and education on how to identify and report scams. In addition, it is imperative that law enforcement bodies in West Africa take their duty to protect citizens seriously and provide impartial and effective assistance in cases like this.

The idea that the Internet is a lawless and unregulated space is a common misconception. In reality, the laws that apply in the offline world also apply to the online world. User behaviour is a focus of laws and regulations in all countries. However, there are various reasons why criminal behaviour is less regulated online in practice (Dutton, 2011). Some of the simpler regulatory measures that work offline, such as zoning, age restrictions, and proof of identity requirements, are more difficult to implement online. Furthermore, there is the challenge of managing and allocating law enforcement resources online and the complexity of harmonising cross-national variations in laws and penalties. Participant KII7 revealed the structural constraints particularly in law enforcement in Nigeria in rooting out digital crimes as their mandate clearly indicates in the various existing national-level policies. The respondent reported endemic corruption in the police department which not only defeats the fight against digital crimes but allows law enforcement agencies to extort money from cybercrime victims (see Box 5.2).

The regulations in response to digital security issues, such as child sexual abuse images, vary among countries. Some countries still lack legislation that specifically addresses this issue. Even in countries that have strong domestic legislation that requires the removal of such material, dealing with images hosted on servers located in other countries is a significant challenge (ICMEC, 2010; Dutton, 2011).

Countries around the world are in competition to attract companies, and research suggests that many nations have chosen to have weaker privacy regulations as a strategic move to gain a competitive advantage over other developed economies. This is often done by smaller countries that have decided to become regional centres for the high-tech industry. This competition seems to imply that the competition on privacy policies among countries is, at least in part, driven by transnational corporations (UNESCO, 2012).

Moreover, the consequences for not following regulations vary; some countries only impose fines for noncompliance, while others can revoke a company's legal authority to handle personal data or may hold noncompliant companies criminally responsible. For example, variations in the data protection laws in Mali, Mauritius, Nigeria, and Togo illustrate the distinctions in how personal data is defined, the rights of data subjects, and the responsibilities of data controllers and data processors (Daigle, 2021).

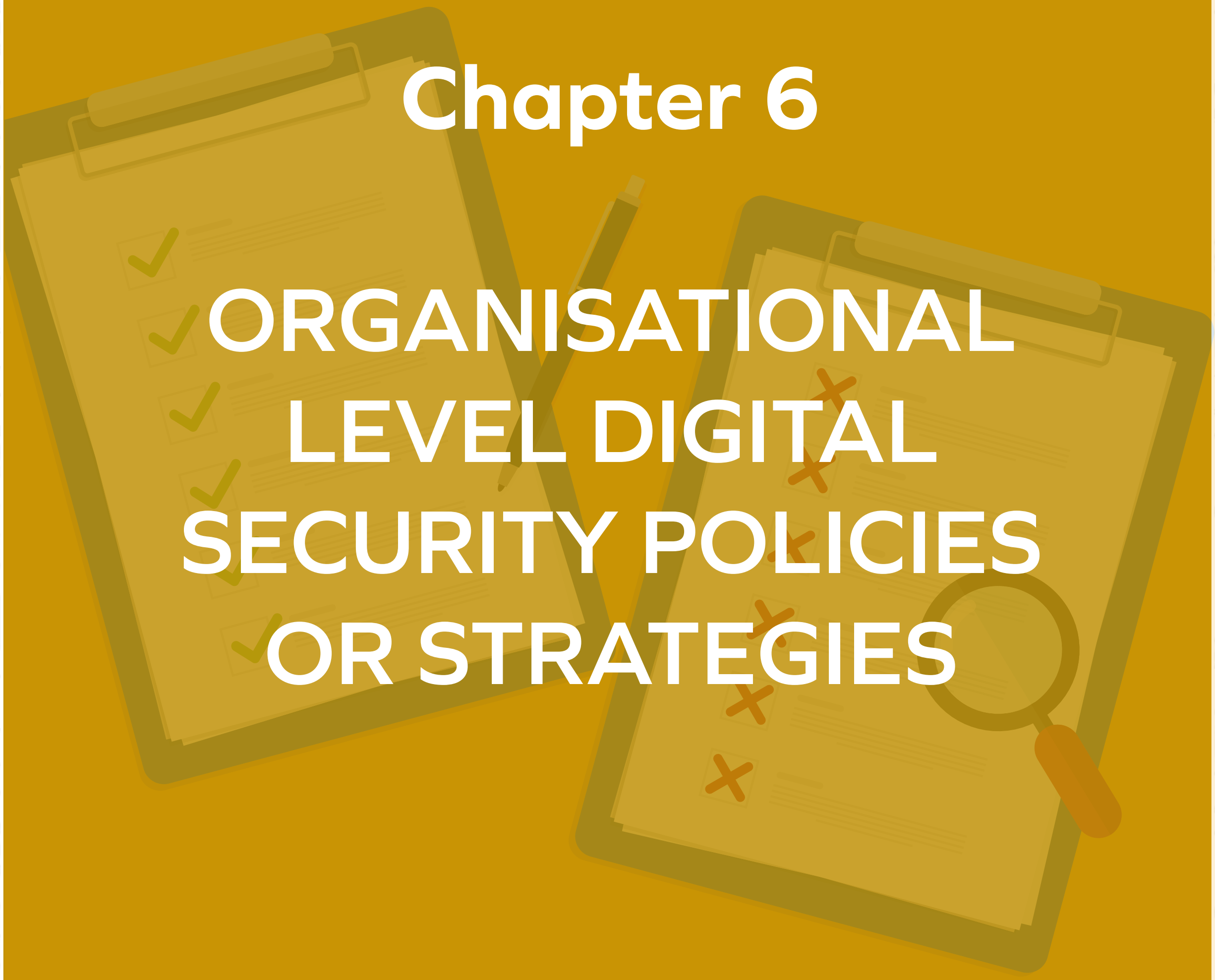
More specifically, the following are some of the gaps and weaknesses in the digital security policies and legal frameworks in West Africa:

1. The lack of specific legislation addressing cybercrime issues in Liberia leaves the country vulnerable to cyber-attacks which hinders efforts to combat cybercrime effectively.

2. Mali's Law n° 2019-056 on the Suppression of Cybercrime contains provisions that may pose potential risks to privacy and freedom of expression online, which could undermine the rights of individuals and restrict the development of the technology sector.
3. The absence of an official national or sector-specific cybersecurity framework in Guinea-Bissau could lead to a lack of clarity and coordination in the country's efforts to protect against cyber threats.
4. In Cameroon, the penalties for violating data privacy are relatively low, which may not be sufficient to deter companies or individuals from engaging in activities that violate data protection laws.
5. The lack of ratification of the African Union Convention on Cybersecurity and Protection of Personal Data by some countries, including Benin, Côte d'Ivoire and Nigeria limit the ability of these countries to collaborate effectively with international partners on cybersecurity issues (see AU, 2023).

Chapter 6

ORGANISATIONAL LEVEL DIGITAL SECURITY POLICIES OR STRATEGIES



This chapter focuses on the organisational-level digital security policies and strategies implemented by the CSOs in West Africa. It analyses the extent to which these organisations adopt and implement policies aimed at protecting their online safety, the usage of personal and organisational devices, remote working, and their overall attitudes towards digital security.

Key Insights

68%

of the sampled CSOs have **NO ICT POLICY** in place in their organisation.

69%

of the respondents **USE** their **OWN** personal **DEVICES** for official tasks or work.

83%

of respondents **AGREE** that attention to digital security is needed in their organisation.

Use of personal devices for performing official tasks

Lucchetti (2018) has shown that many organisations in West Africa lack structured strategies for tackling digital threats due to a shortage of ICT employees. The few ICT staff employed are often not adequately trained to draft organisational digital security frameworks, and lack the skills to provide technical support that can successfully detect, manage, and prevent the occurrence of digital threats. Furthermore, the absence of effective national digital security policies and regulations in most African countries (as shown in the previous chapter) is a disincentive to developing organisational security policies. This is because the lack of a national digital security policy fails to create the necessary awareness among organisations of the need to develop and implement their own online safety strategies. Consequently, there is a common pattern of using personal digital devices for performing official tasks at work in organisations without organisational-level digital security policies. The data from this study supports this assertion.

The survey results shown in Figure 31 suggest that a significant share of CSOs in West Africa use their personal digital devices for work. Specifically, 69% of the respondents indicated that they use their own devices, while 62% reported using devices provided by their organisation. It is worth mentioning that some staff use both personal and official devices to perform their work, hence the overlap in the proportions. Additionally, 13% of respondents reported sometimes using other people's devices.

This suggests that there is a high level of flexibility in terms of device usage among CSOs in the region. However, this also highlights a potential security concern as personal devices may not have the same level of security measures in place as organisation-provided devices.

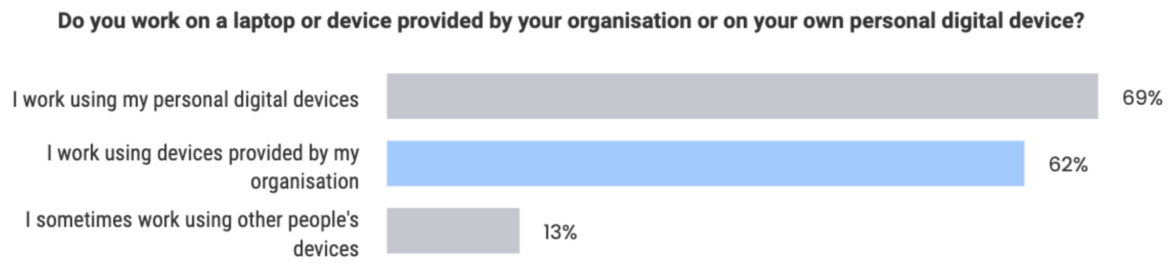


Figure 31: Use of Personal Devices for Performing Official Tasks / Source: WACSI (2023)

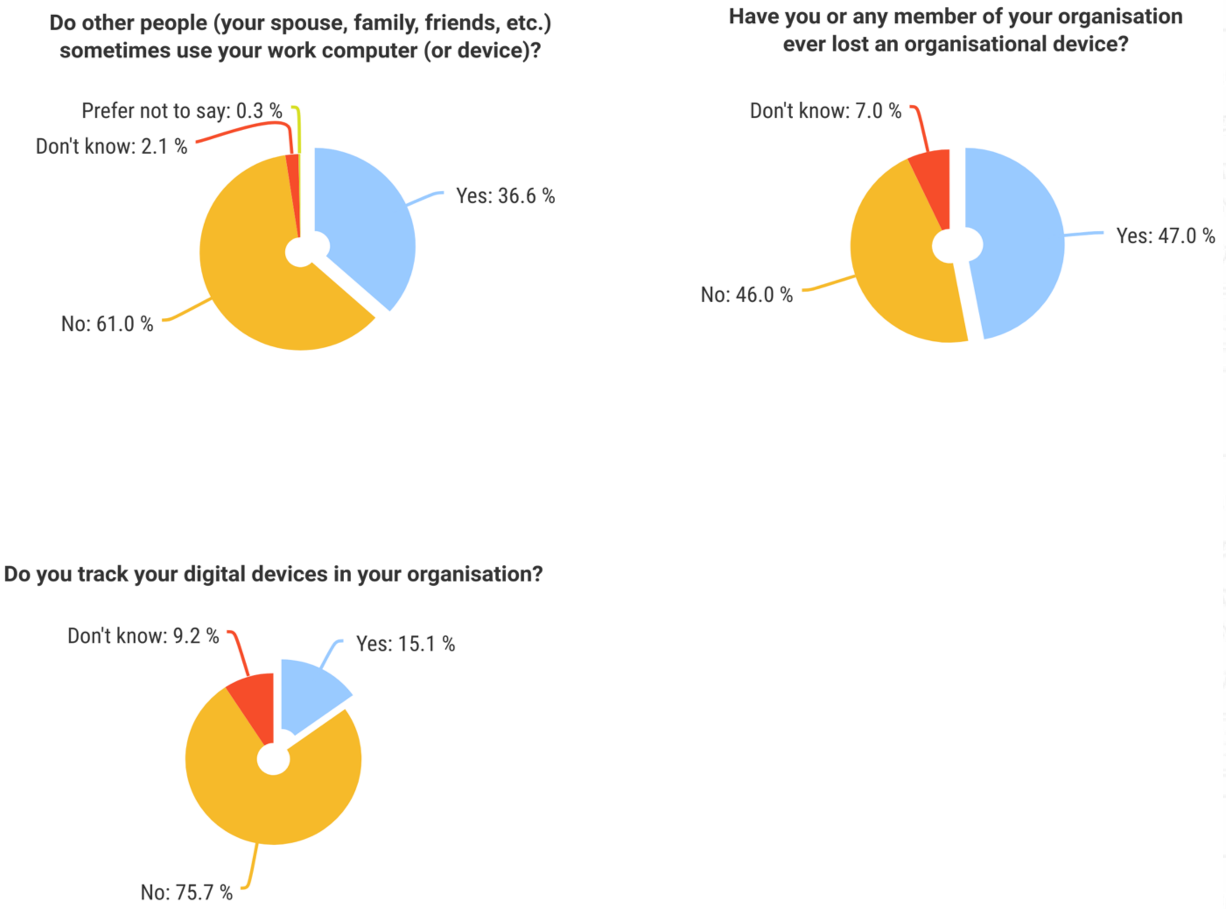
Additionally, the use of other people's devices can also increase the risk of security breaches, as the devices may not be properly secured. This emphasises the need for CSOs in West Africa to have clear device usage policies in place and to ensure that all devices are properly secured to protect them against digital security threats.

Use of organisational devices for personal work

Interestingly, employees of CSOs were not only found to be using their personal digital devices in completing official tasks but also, they allow their acquaintances to sometimes use their official digital devices for personal online activities. The survey data for this study further presents data on the tracking of organisational digital devices as well as loss of organisational digital devices.

The results show that approximately 37% of respondents indicated that other people such as friends, family, or their spouses sometimes use their work devices, which complicates the security of their digital devices since sensitive data on the work devices may be exposed to people outside the organisation.

Also, many of the sampled CSOs are not tracking their digital devices. Only 15.1% of respondents reported that they track their devices, while 75.7% said that they do not. This suggests that many CSOs in the region are always not aware of the locations of their devices and may not be able to respond quickly if a device is lost or stolen. Moreover, the high percentage of respondents (47%) who reported that they or a member of their organisation have lost a device, highlights the importance of device tracking and management, all of which form an integral part of organisational level ICT policies, which most of them do not have.



Do other people (your spouse, family, friends, etc.) sometimes use your work computer (or device)?

Have you or any member of your organisation ever lost an organisational device?

Do you track your digital devices in your organisation?

Figure 32: Digital Device Management in CSOs / Source: WACSI (2023)

This lack of device tracking, coupled with the high usage of personal devices, create security vulnerabilities, as lost or stolen devices may not be reported or tracked, making it difficult to protect sensitive data stored on the devices. These results imply that CSOs in West Africa are at a higher risk of data breaches and other security incidents due to the lack of strict policies and procedures for the use of digital devices and lack of device tracking and management. The results also imply that CSOs in the region are at a high risk of losing sensitive data or confidential information if a personal device is lost or stolen.

Participant KII15 from Côte d'Ivoire points to breaches of confidential information in their organisation, emphasising the need for organisational level policy in promoting digital safety among CSOs (see Box 6.1).

Box 6. 1: Defend Your Inbox! / Source of excerpt: KII15

CASE STUDY

We are a local NGO in Côte d'Ivoire, and we work to promote health and economic and social development with an emphasis on vulnerable populations, namely women, children, and young people. I received an email in April 2022 stating that someone tried to access the organisation's email. The message asked if it was me, and if not, to click on "it's not me" to change the password. As I had given the password to only two people, I called them to inquire if they were trying to log in with the email, but they said no. So, I immediately changed the password and shared it with the three authorised personnel for the organisation's email.

Additionally, I lost access to my personal email account. When I tried to sign in, I was asked to enter the emergency address. The backup address that was presented was not the one I had originally set up. As a result, I lost my email address. When I tried to reset my password, I was asked for my password. But when I entered it, the password was incorrect. When I selected the "forgotten password" option, I was taken to my secondary email address, but the secondary address was not the one I had used to set up the account. I lost the email account.

The excerpt above is from a key informant interview with a CSO in Côte d'Ivoire and the security issue experienced was a hacking attempt. The informant received an email notification that someone had tried to access the organisation's email address. The informant immediately changed the password and shared it with the authorised personnel. However, the informant also lost their personal email address as they were unable to access it and the secondary email address provided was not what they had set up. This case offers several learning opportunities for CSOs in West Africa:

Importance of password management: **Organisations must have proper password management protocols in place and regularly change their passwords to prevent unauthorised access**.

Awareness and training: CSOs should train their staff on digital security and awareness on how to identify and prevent hacking attempts. Providing training and awareness to staff on best practices for digital security can also help ensure that everyone in the organisation is taking the necessary precautions to protect the organisation's assets.

Importance of IT support: Having IT personnel or external IT support can provide better digital security measures and protection against hacking attempts.

Backup email address: CSOs should ensure that the backup email address is up to date and that they have access to it in case of any emergency.

Security notifications: CSOs should take security notifications seriously and act promptly to prevent any potential harm.

Ultimately, having an organisational level digital security plan or policy and implementing it effectively can help address many digital security challenges such as those faced by the CSO in this excerpt. Such a plan should include regular password changes, setting up secure backups for important data and communications, and having a clear process for managing access to the organisation's email and other digital accounts. By implementing these measures, CSOs can reduce the risk of unauthorised access, minimise the impact of lost or stolen passwords, and ensure the continued security of sensitive information.

Working from home and seeking digital security

The recent trend of remote work, including working from home, has brought new challenges to digital security for CSOs in West Africa. To mitigate digital attacks, it is essential to adopt strategies such as using Virtual Private Networks (VPNs) while working remotely. The study explored these challenges and their impact on CSOs' digital safety, as reflected in Figures 33 (a and b). The research findings show that 92.9% of CSOs in the region occasionally work from outside the office, including their homes and other remote locations. This trend is primarily driven by the need for flexibility and mobility among CSOs, as well as the COVID-19 pandemic's impact on remote work.

However, this trend also highlights the potential digital security gaps among CSOs in West Africa. The study found that only 26.5% of respondents use VPNs while working remotely, leaving a significant number of CSOs at risk of unsecured connections and potential cyber-attacks. The adoption of VPNs creates a secure connection to the organisation's network, encrypting data and safeguarding it against potential threats such as hacking and snooping. The low adoption of VPNs among CSOs in West Africa underscores the need for more digital security training and awareness campaigns in the region.

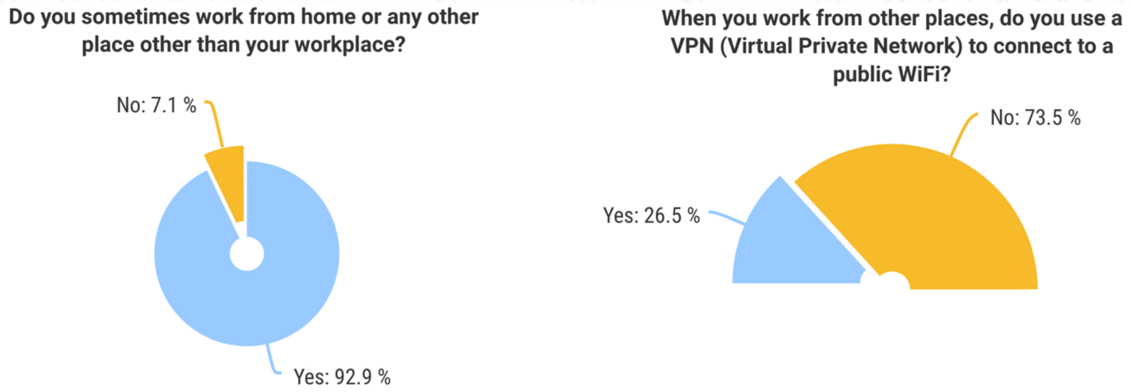


Figure 33: Working from Home

Many CSOs lack awareness of the need to develop and implement their own online safety or digital strategies. The lack of such policies contributes to poor digital security practices and negligent behaviour among CSO staff, as seen in the case of KII23 in Box 6.2 where the CSO's digital system was hacked. Despite acquiring antivirus licenses, the participant noted that their organisation was negligent in changing passwords, emphasising the importance of implementing effective organisational level digital security policies and promoting awareness among CSO staff.

Box 6. 2: When Hacking Strikes – The Price of Neglecting IT / Source of excerpt: KII23

CASE STUDY

The digital security experienced by the CSO in West Africa as described in the excerpt is a breach of their email account. The email account was hacked three years ago, and the CSO was unable to regain access to it. The CSO later created a new email address and assigned a single person to manage it, but they did not have any special computer security measures in place. The CSO only realised that they had been hacked when they received reports that they had sent messages asking for money. After the incident, they bought antivirus licenses to improve their security but they still do not change their passwords regularly. The CSO does not have an IT manager or someone equipped to take care of their computer security.

It has been three years now and we still cannot access our email address. It appears that someone hacked into our email and despite our efforts, we have not been able to retrieve it. During that time, we had to manage without it. We created a new email and assigned one person to manage it, but there were no special computer security measures in place. We only realised that there was a problem when people told us they received messages requesting money from us that we did not send. We tried to access the email but could not. After that, we purchased antivirus software licenses for better protection, … but we do not change passwords regularly. We do not have an IT manager or someone equipped to take care of these issues.

The experience of this CSO highlights a key challenge facing CSO: not having an IT unit or personnel to handle digital security within an organisation. The lack of specialised personnel in the CSO led to a situation where the email account was hacked and used for malicious purposes. The CSO only realised the security breach when people reported receiving messages asking for money. This shows the importance of having measures in place to detect potential security breaches. Moreover, the experience highlights the need for training and awareness among staff to ensure proper digital security practices are implemented. The lack of regular password changes, and the absence of an IT manager shows a lack of attention to digital security measures, which is essential for CSOs to protect their critical information and communications. CSOs in West Africa that use ICTs in their operations should prioritise the establishment of IT units and invest in training and awareness programs to improve their digital security posture. This would reduce the likelihood of security breaches and protect the CSOs' sensitive information, communication and operations.

CSOs' Attitudes toward Digital Safety

Examining CSOs' attitudes towards online safety is crucial for understanding their preparedness in achieving digital safety. This analysis can provide valuable insights into their awareness levels of digital threats, as well as their willingness to adopt digital security technologies (see Figure 33).

The survey results suggest that CSOs in West Africa have a generally positive attitude towards digital security. A high percentage of respondents (72%) believe that they can protect their digital devices from harm if they try. Additionally, most respondents (83%) believe that attention to digital security is needed in their organisation. However, a significant percentage (26%) of respondents also agree that their efforts make no difference, and that people will still hack them if they want to. This suggests that despite having a positive attitude towards digital security, some CSOs may have a sense of resignation or helplessness towards protecting themselves from digital threats. Also, a relatively low percentage (15%) of respondents believe that they do not have sensitive data to be worried about. This implies that some CSOs may have a lack of understanding or awareness of the types of information they possess that may be valuable to cybercriminals. Therefore, CSOs in West Africa may benefit from increased education and training about digital security risks and best practices, as recommended in Chapter four.

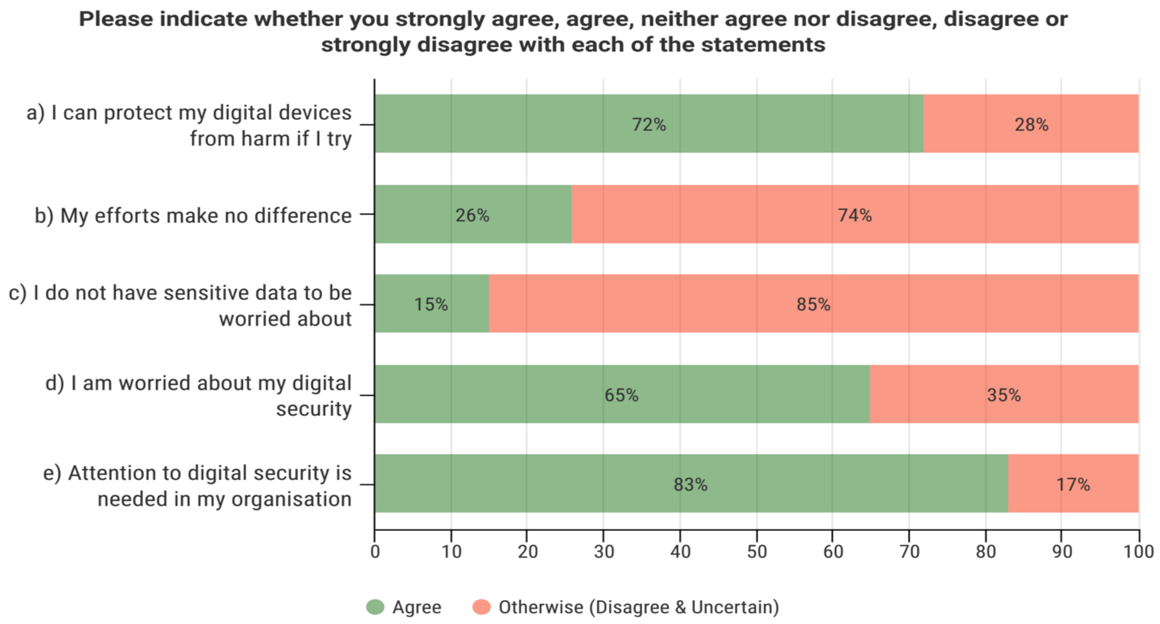


Figure 34: CSOs' Attitudes toward Digital Safety / Source: WACSI (2023)

Digital Security Policy Adoption among CSOs in West Africa

Digital security policy adoption among CSOs in West Africa is a critical aspect of ensuring the safety and privacy of their data and information. However, it is often challenging for CSOs to adopt digital security policies due to limited resources, capacity, and technical expertise. As shown in previous chapters and the above sections in this Chapter, many CSOs in the region lack awareness of the potential risks and threats they face in the digital space, as well as an understanding of the importance of adopting digital security policies.

The survey revealed that only 26.4% (see Figure 35) of the sampled CSOs have a computer and information security policy

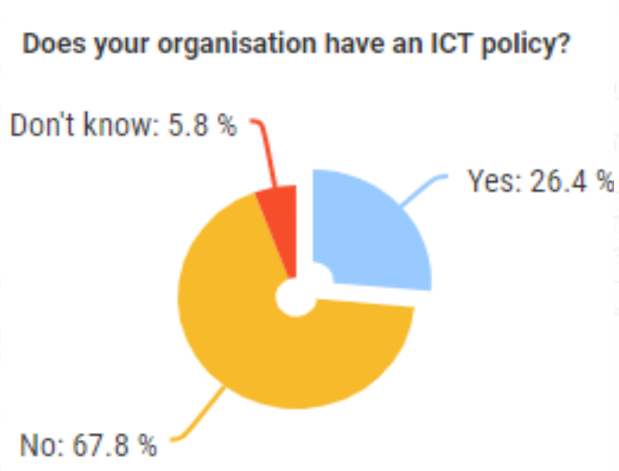


Figure 35: CSOs Having Digital Security Policy / Source: WACSI (2023)

in place, an indication that a large majority of the CSOs are not taking the necessary steps to protect their digital assets and operations. Without a clear policy in place, CSOs may be more vulnerable to digital security threats and may be less able to respond to incidents effectively.

Of the CSOs that reported having a policy in place, 71% reported that they are aware of the contents of the policy, suggesting that while some CSOs have a policy in place, their staff may not be fully cognisant of its contents and how to apply them. This lack of knowledge can make it difficult for CSOs to implement and enforce the policy, leaving them vulnerable to digital security threats.

When asked if they understand the contents of the policy, 76% of the respondents said yes, again suggesting that a significant portion of the CSOs (24%) reported not understanding the contents of the policy. This implies that the policies may not be communicated effectively to all members of the organisation, and staff may not have the necessary knowledge to implement them.

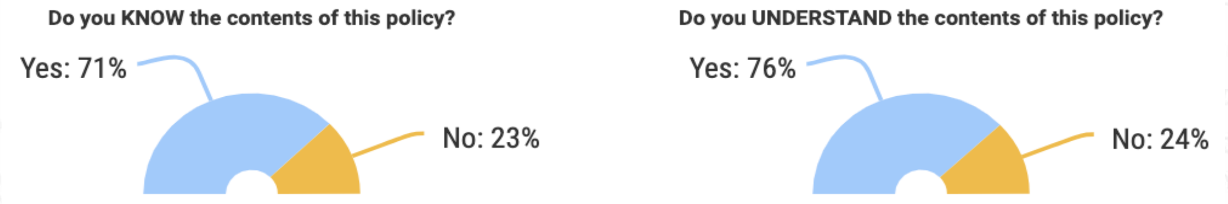


Figure 36: CSOs' Knowledge & Understanding of Digital Security Policy / Source: WACSI (2023)

Apart from a significant portion of respondents not knowing or understanding the contents of their organisation's ICT policy, 27% of them admitted to deviating from the requirements of the policy, and the same percentage of respondents believing that their colleagues also deviate from the policy. This implies that there is a lack of understanding and adherence to the policy which can lead to vulnerabilities and breaches.

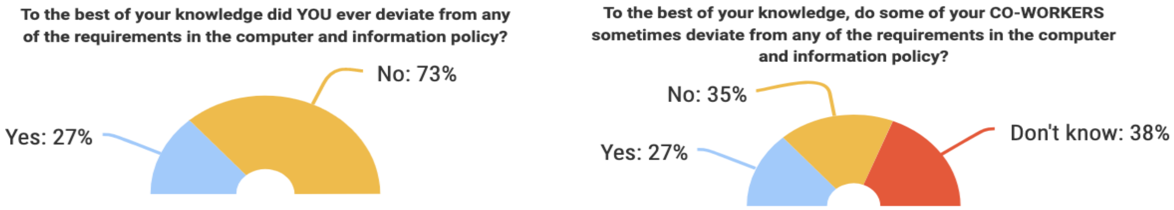


Figure 37: CSOs' Deviation from Digital Security Policy / Source: WACSI (2023)

The results highlight the need for CSOs in West Africa to have a clear and comprehensive computer and information security policy in place, as well as training for employees to understand and adhere to the policy. This can help to reduce the risk of digital security threats and protect the organisation's sensitive data. The call for organisational level digital security policy is emphasised by participant KII16 as Box 6.3 demonstrates.

Box 6. 3: A Call for Digital Policy / Source of excerpt: KII16

CASE STUDY

We do not currently have a digital security policy because we lack an expert who can help us draft one and guide us on best practices. I believe that having such a policy would make a significant difference in protecting our organisation's digital assets. For example, we could implement measures to block certain websites that are prohibited for staff to visit with the organisational internet.

When I worked at Plan International, they had strict policies in place that prevented access to certain websites on office laptops. I think these kinds of restrictions could be implemented by an IT person if we had a digital security policy in place.

The excerpt above highlights the need for CSOs in West Africa to have a digital security policy in place. The informant, a top official in a local NGO in Nigeria, mentions that their organisation does not currently have a digital security policy, and they lack sufficient knowledge and resources to draft one. The informant recognises the importance of having such a policy, as it can help to restrict access to certain websites and prevent staff from potentially accessing harmful or prohibited content while using organisational technology. It is imperative for CSOs in the region to consider the importance of having a clear and comprehensive digital security policy to ensure the protection of sensitive information and secure use of technology. Without a policy in place, organisations may be at a higher risk for digital security breaches and compromise of sensitive information. CSOs in West Africa should prioritise finding an expert in digital security to help draft a policy and ensure that all staff members are aware of and understand the policy. Implementing a digital security policy can make a great difference in protecting organisational assets and maintaining the privacy and security of sensitive information.

Chapter 7

THE MAJOR DIGITAL SECURITY CHALLENGES FACING CSOs IN WEST AFRICA

Major Challenges Facing CSOs Regarding Their Digital Security and Safety

Effective digital security requires a multifaceted approach that addresses the institutional, technological, political, economic, psychological, and legal challenges facing CSOs in West Africa. The increasing use of digital technologies in CSOs' operations, coupled with the growing dependence on them, has made them more vulnerable to digital security threats. Cybercriminals can easily steal sensitive information, disrupt operations, or spread misinformation using social media, messaging apps, and online platforms.

However, challenges to digital security go beyond cyber-attacks; physical attacks and seizure of digital data storage devices are also concerns. According to Henrichsen et al. (2015), achieving significant digital security requires state power, an organisation's digital policy, and the conduct of individual employees to work cohesively. Nevertheless, CSOs' digital security posture is often hindered by limited resources and expertise, making them easy targets for cybercriminals.

Many employees also perceive some online security technologies as unfriendly to use, leading to a situation where few employees appropriately use them, and many others ignore them entirely. Phishing and spear-phishing attacks targeting CSOs' social media and messaging apps are prevalent, and these attacks can steal sensitive information or spread malware. Effective digital security requires a comprehensive approach that addresses the various challenges facing CSOs in West Africa.

Due to limited resources and capacity, many CSOs in West Africa are increasingly vulnerable to digital security attacks. Limited funding and personnel make it difficult for CSOs to implement effective cybersecurity measures, such as investing in cybersecurity software, hardware, and services. In addition, many CSOs lack the technical expertise necessary to identify and respond to cyber threats. This limited capacity also applies to managing and maintaining cybersecurity systems, providing training and awareness programmes to staff, and upgrading digital security technologies. Consequently, CSOs are often exposed to digital security risks. As participant KII17 noted (see Box 7.1), the anxious desire among CSOs to solicit adequate funding to finance their projects further exacerbate their vulnerability to online attacks.

Box 7. 1: The Deceptive Donation Dilemma / Source of excerpt: KII17

CASE STUDY

An acclaimed funder contacted me claiming to be from outside the country. They sent me a letter stating that they are a charity organisation and that they have seen me on a platform doing some work in the country. They said they would like to fund our organisation to carry out more work in the country. I was thrilled and sent all the information they needed, but till this day, I have not received any information from them. I am not sure what they used the information for, but it's clear they used it for something. I later realised that I was not supposed to send information like that without first checking the authenticity of the request. They asked for our certificate of incorporation, organisational profile, and bank account details. I sent it to them because genuine funders usually want to see those things, but I learned a lesson. I must now check first if someone requests information from our organisation.

This excerpt highlights a common issue faced by CSOs in West Africa when dealing with potential funders: the risk of falling victim to fraudsters posing as genuine funders. The informant in the interview sent information, including the organisation's certificate of incorporation, organisational profile, and bank account details, to a supposed funder who had contacted them. However, no further information or funding was received, leading the informant to believe that the information was being used for malicious purposes. This has several implications for CSOs in West Africa such as the following:

◊ **Vulnerability to fraud**: CSOs in West Africa are at risk of falling victim to fraudsters who pose as genuine funders and request sensitive information.

◊ **Importance of due diligence**: CSOs need to be cautious and perform thorough due diligence before releasing any information to potential funders.

◊ **Awareness of information security**: CSOs should be aware of the importance of protecting sensitive information, such as bank account details, and not releasing it without proper verification.

◊ **Need for proper information management**: CSOs should have proper systems in place for managing and protecting sensitive information, including data protection policies and procedures.

◊ **Importance of training and capacity building**: CSOs in West Africa should prioritise training and capacity building on digital security and information management to better protect themselves and their stakeholders from potential threats.

Overall, the experience highlights the need for CSOs in West Africa to be proactive in protecting themselves from digital security threats and to be vigilant in verifying the authenticity of potential funders before releasing sensitive information

As aforementioned, CSOs in West Africa face significant challenges in maintaining their digital security due to their limited resources and capacity. This creates difficulties in conducting regular security assessments, penetration testing, and incident response planning, which is critical in identifying vulnerabilities and responding to digital security attacks. CSOs that rely on foreign funding tend to be more vulnerable to digital security attacks, as cybercriminals often target their sensitive information, such as financial records or donor information, or seek to disrupt their operations. Highly dependent foreign-funded CSOs are perceived as soft targets by cybercriminals due to their need for external funding opportunities and their limited protection against cyber-attacks.

Poor digital infrastructure among CSOs in West Africa has also been identified as a significant challenge to digital security. Many CSOs in the region lack the necessary digital infrastructure to adequately secure their systems and data. These include outdated hardware and software, inadequate firewalls and antivirus software, and limited technical expertise to manage and maintain digital security systems. Such weaknesses make these organisations vulnerable to cyber-attacks and data breaches. As stated by participant KII18, the lack of adequate digital infrastructure among CSOs in the region is a significant concern that hinders their ability to maintain digital security (see Box 7.2).

Box 7. 2: The Struggle: No laptops, Unsecured desktops, No Internet / Source of excerpt: KII18

CASE STUDY

We lack an IT person to be solely in charge of IT in the organisation. When officers return from the field, we are dealing with only two desktop computers since the laptop is not always available. Whenever the officers bring data from the field, they come and sit in front of the computer to work. Additionally, we don't always have internet facilities. Sometimes I use my hotspot to connect to my desktop, and other times we go to a café. We only have two pen drives for the organisation, so any officer can just take one and go to the café, especially on weekends. Sometimes, when they come back on Monday, they just insert the pen drive to work. However, sometimes the system hangs, and we have to restart the computer to gain access to the information. We also lack the knowledge to put passwords on our documents. Although there is a young guy here who used to do it for me, he has left. Any officer can sit by the computer and copy any information they want. Additionally, officers' friends sometimes come to the office, and some of them may be allowed to sit by the computer to do something. All of our documents are not password-protected.

The excerpt above is from a key informant interview with a CSO in Ghana highlighting several challenges to digital security among CSOs in West Africa. Firstly, the lack of an IT person solely in charge of IT in the organisation creates a gap in the proper management of digital security. Secondly, the lack of an internet facility forces staff to resort to using their personal hotspots and visiting cafes to access their data, which increases the risk of data exposure and theft. Additionally, the unavailability of laptops, limited number of desktop computers, and the lack of knowledge about password protection makes it easy for anyone to access sensitive information stored on the computers. The use of pen drives, where information is copied and taken outside of the office, also increases the risk of data exposure and theft.

These challenges pose serious implications for the security of CSOs' sensitive information in West Africa. To overcome these challenges, CSOs in West Africa need to invest in proper IT infrastructure, including laptops and desktops with internet facilities, and appoint an IT person to manage the digital security of the organisation. Additionally, providing training and education on basic digital security practices such as password protection, data encryption, and secure data transfer methods is critical in reducing the risk of data exposure and theft.

CSOs in West Africa that work on sensitive or controversial issues such as human rights, political activism, or environmental issues are particularly vulnerable to cyber-attacks due to the nature of their core activities. These CSOs are often targeted by cybercriminals and state-sponsored actors who use cyber-attacks as a form of espionage, censorship, or repression. For example, cybercriminals may launch spear-phishing campaigns on CSOs to steal sensitive information or launch Distributed Denial of Service (DDoS) attacks to disrupt their operations. Some state-sponsored actors use malware or spyware to monitor the activities of CSOs and steal sensitive information. Also, CSOs that are involved in sensitive or controversial issues often become the target of online disinformation campaigns designed to spread false information and undermine their credibility. These sometimes result in financial losses for CSOs, as attacks that censor their websites by denying access to visitors lead to a loss of services on the site. Key informant KII9 provides a typical case of a cyber-attack in Niger that spread misinformation about a planned protest by their CSO, demonstrating the reality of these types of attacks in the region.

Box 7. 3: False Alert! Source of excerpt: KII9

CASE STUDY

This highlights a case of cyber-attack and misinformation experienced by the CSO in Niger. As described in the excerpt below, the network coordinator's account was hacked and used to spread false information about a planned protest march. This created confusion among citizens and threatened the success of the planned demonstration. The CSO was able to quickly respond by providing accurate information through backup messages, using the media, and setting up mock designs to get the word out.

We mainly work on four strategic axes: peace and security, democracy and good governance, sustainable development as the third axis, and leadership of young people and women as the fourth, which we focus on. A few months ago, as part of our citizen mission, we planned a protest march against certain measures taken by the government. Unfortunately, the network coordinator's account was hacked and used to disseminate messages that stated that "the march no longer holds". Fortunately, we were able to retrieve the account, and then inform the citizens that the messages were the result of hacking. We filed a declaration of demonstration in the city of Niamey, and the declaration was accepted, and the march was authorized. A few hours before the march, parallel accounts were created by supposed presidents of our organisation to inform people that the march was no longer taking place. We had to create models, designs and use the media to properly inform the citizens.

When asked how they detected the security bridge, the informant continued,

It was through a message. When, for example, friends called us to ask us if it's true that the march had been cancelled again. Then we understood that there was a false profile spreading false information… it was astonishing, I was surprised. Well, we quickly put in place a mechanism to be able to truly overcome the inconvenient.

This situation highlights the importance of digital security and the need for CSOs to be aware of the potential threats posed by hackers and cyber criminals. Additionally, it shows the importance of having a plan to respond effectively to security breach, as well as the importance of regularly reviewing and updating digital security measures to ensure the protection of sensitive information. Lamenting on the potential causes of such a security bridge, the key informant added,

The threats are that civil societies are perceived by the state as a kind of opposition. It's a threat to the authorities because there's information, they don't want out there. There are also hackers who hack accounts, put viruses, and set up antivirus mechanisms to buy. There are all these parameters.

The key informant believes that the cause of the security breach experienced by their organisation is due to the perception of CSOs as opposition to the state, which makes the information that these organisations have potentially threatening to the authorities. Also, the informant mentions that there are also external actors such as hackers who can compromise the security of the organisation's digital assets by hacking into their accounts, putting viruses, and selling antivirus mechanisms. These various factors pose a threat to the digital security of CSOs in West Africa. CSOs need to be proactive in protecting their digital assets, including being aware of the potential threats they may face, and taking appropriate measures to mitigate those threats, such as implementing robust digital security policies and training staff on safe digital practices.

Countries in the West Africa region with a history of political instability and human rights violations create a challenging environment for civil society to operate. CSOs in these countries face various forms of attacks not only in the digital realm but also in the physical world. These attacks can manifest in various ways, including harassment, intimidation, arbitrary arrests, and physical assaults, as discussed in Chapter two, and Chapter five (in the case of repression in the civic space). In some cases, the physical attacks are linked to digital security threats, such as cyber espionage or online disinformation campaigns. Government surveillance, restrictions on freedom of expression and association, and the use of force against activists and CSOs are some of the common challenges that CSOs in the region face. A participant, KII14, provides a classic example of a CSO member who was targeted and physically assaulted by an unknown individual, in connection to the work of their organisation.

CSOs in West Africa are facing the challenge of inadequate digital security training or skills among their staff. Many CSOs lack the necessary expertise to identify and respond to cyber threats, and their staff may not have the technical skills and knowledge necessary to manage and maintain cybersecurity systems or provide training and awareness programmes to their colleagues. This lack of digital security training or skills is largely due to the limited financial resources available to many CSOs in the region. Without adequate funding, it becomes challenging for these organisations to set up proper digital systems to protect their operations online. Respondent KII4 lamented their CSO's lack of digital sophistication, highlighting the inadequacy of their digital training and the lack of enough funding to invest in cybersecurity measures to protect their online operations effectively.

Box 7. 4: Targeted and Beaten: The Perils of Advocacy / Source of excerpt: KII14

CASE STUDY

The following case describes a physical attack on a helpline counsellor from a foundation based in Nigeria, who is the first respondent to children reporting cases of child sexual abuse or physical abuse. The attack occurred after the helpline counsellor received a call from a child and introduced the name of their organisation to the caller. A man who alighted at the same bus stop as the helpline counsellor later attacked the counsellor, mentioning the name of their boss and a case the organisation had handled.

I work with a foundation based in Nigeria that helps children aged 0 to 18 who have been sexually abused or are at risk of being abused. I am a helpline counsellor at the foundation, responding to children who call to report cases of child sexual abuse or physical abuse. It's a 24-hour helpline, so children can call at any time to report cases of abuse. One day in January this year, after work, I picked up a call on the bus, as it's normal for us to do so when calls are persistent. As a helpline counsellor, it's standard practice to introduce the name of our organisation, which I did. Later on, I noticed that a young man had alighted at the same bus stop as me and was walking directly behind me, but I didn't think much of it. When I got to a quiet place, he pulled me from behind, slapped me, and started mentioning the name of my boss. I told him that I was not the person he was looking for, but he said that he would deal with me and then go back to the office to tell my boss what he had done to me. He rough-handled me, pulled my hair, and hit me. Luckily, some people gathered and witnessed the incident, asking why he was beating his wife and telling him to leave me alone. I told them that I was not his wife and that I didn't even know him. He then began explaining a case that my organisation had handled, mentioning sensitive names and the fact that this person was very popular in Lagos, Nigeria. He said that this organisation had jailed his elder brother. In the end, I was able to escape and ran into a church where I sat down for a while. Then I called someone who was close to me to come and rescue me, and I also informed the office of what had happened. The office reported the case to the police station, and the case was documented. The police assured us that investigations would be carried out to protect us and other people in the organisation.

The attack experienced by the helpline counsellor highlights the dangers of having work-related conversations or talking about sensitive topics in public without being aware of one's surroundings. The victim, who was a first responder to children reporting cases of child sexual abuse or physical abuse, may have revealed information in the course of answering a call on a public transport that caught the attention of the attacker. It is possible that the attacker was pursuing the victim even before the victim picked the call, or that the attacker was related to someone whose case was previously handled by the organisation and happened to be in the same public transport with the counsellor. Regardless of how the attacker obtained the information, the attack serves as a reminder of the need to be cautious when having conversations or talking about sensitive information in public, especially when it is work-related.

The implications for CSOs and others working in sensitive areas are clear. It is important to be aware of one's surroundings and to be mindful of the information being shared when in public. This can include avoiding discussing sensitive information on phone calls in public, or being aware of potential risks and taking steps to protect oneself and others. In addition, it is important for CSOs and others working in sensitive areas to have robust security protocols in place to mitigate the risks posed by such incidents and to ensure that they can continue to carry out their important work effectively and safely.

Box 7. 5: CSO Cybersecurity Challenge: Funding the Fight / Source of excerpt: KII4

CASE STUDY

As the director, my knowledge of digital security is at a basic level and it's the same for the members of our organisation. We have been trying to raise funds to bring someone from Canada to teach us digital security, as I was taught in the US before, to guide and teach us. We are also raising funds to buy computers and phones for everyone to use for work, and we are still in that process. Our organisation has a large number of staff, a national movement, and we have staff all over the country who work on various aspects of our work. We use a lot of Teams and Zoom meetings to be able to work. We really need a lot of security support, and we are still doing what we know personally. We wish to have a more holistic approach to secure all of our systems, and that is why we are raising funds to get computers that can be linked, phones that can be used for work with sim cards, and a server installed with anti-hacking features. This whole process is not cheap, but we are still hoping to find the right donors to support our efforts.

The key informant is the director of a local NGO in Ghana that works to protect human rights and minority groups and also seek to change attitudes and foster acceptance and tolerance of all persons. The organisation is facing several challenges in terms of digital security, including:

◊ **Lack of training**: The director mentions that they have been trying to raise funds to fly in someone to teach digital security as they had limited training before.

◊ **Insufficient technology resources:** The organisation is still in the process of raising funds to buy computers and phones for their staff, which would allow them to use organisational resources for work.

◊ **Large number of staff**: The organisation has a large number of staff members who work from different locations and use Microsoft Teams and Zoom to connect and work together.

◊ **Lack of specialised support**: The organisation requires a lot of security support, but is still relying on personal knowledge and skills, wishing for a holistic training and support.

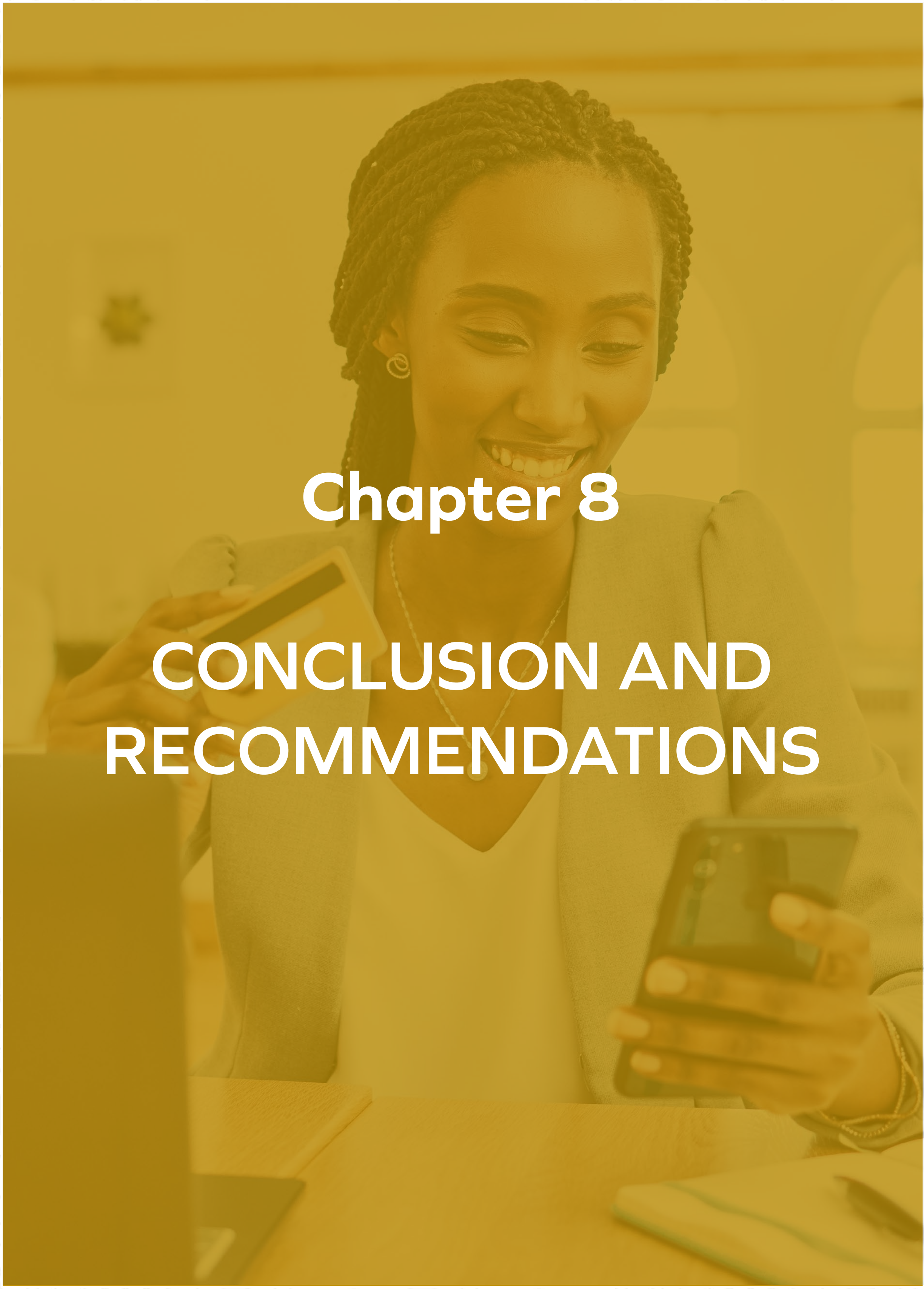
◊ **Cost of implementing security measures**: The director mentions that having a server installed with anti-hacking features, hiring people to monitor it, and using work-only SIM cards for phones is not cheap.

The lack of sufficient training, inadequate resources, and the absence of a comprehensive security strategy all present significant hurdles in securing their digital assets and information. The reliance on personal devices, limited technical knowledge and the use of unsecured networks also expose the organisation to a range of digital security threats. To overcome these challenges, it is essential that CSOs in West Africa prioritise digital security and invest in training their staff, procuring secure devices and networks, and implementing a comprehensive security strategy. A holistic approach to digital security, including the use of security software and regular security assessments, can help mitigate the risk of cyber threats and ensure the long-term stability and security of the organisation.

Finally, at a macro level, countries in the region have limitations in protecting the online safety of their citizens due to inadequate legal and regulatory frameworks. The lack of comprehensive and harmonised digital security legislations, understaffing of law enforcement agencies with digital security capacity, and inadequate data on digital threats or attacks, all contribute to the vulnerability of CSOs to digital security threats. This challenging environment makes it difficult for CSOs to protect themselves or seek justice if targeted by cybercriminals.

Overall, the challenges to digital security among CSOs in the region are numerous and diverse. They include:

1. Inadequate ICTs and digital security infrastructure among CSOs.
2. Low digital security awareness, inadequate training and or limited skills to implement effective cybersecurity measures.
3. Limited funding to invest in cybersecurity, and dependence on donor or foreign funding, making CSOs more vulnerable to digital security attacks.
4. Lack of organisational-level digital security policies or strategies and inadequate implementation where they exist.
5. Repression in the civic space in the case of CSOs involved in sensitive or controversial issues, such as human rights, political activism, or environmental causes, particularly vulnerable to cyber-attacks.
6. Inadequate legal and regulatory framework in many West African countries to effectively address cybercrime and protect citizens' rights online.
7. Lack of harmonisation of digital security legislations among law enforcement agencies in many countries.
8. Understaffed law enforcement agencies with very few or no staff with digital security capacity to support investigations of digital threats or attacks against CSOs.
9. Lack of publicly available data to study the prevalence, determinants and effects of digital threats or attacks against CSOs.
10. Limited capacity or resources to investigate and prosecute cybercrime in some countries, which creates an environment that is conducive to cybercrime.



Chapter 8

CONCLUSION AND RECOMMENDATIONS

Conclusion

CSOs are increasingly employing digital technologies in their operations as well as having a high appetite for digital security training due to their experience with various types of digital security attacks. This report has highlighted the multiplicities of major digital security threats confronting CSOs in West Africa and the policy issues striving to shape the nature of digital activities and curb digital security crimes.

There is a high prevalence of digital security threats and/or attacks among CSOs in West Africa, following their increasing use of ICTs, even though these threats or attacks manifest differently across countries and by CSO type. With a staggering 31% of CSOs in West Africa reporting having experienced a digital security attack in the last year, the digital security landscape in the region is far from ideal. From computer virus attacks to threats through social media and email, these organisations are facing a variety of digital security challenges. The results showed Nigeria leading the pack with 10.75% of the attacks, with Ghana following closely behind. Unfortunately, these attacks are not just a one-time occurrence, with at least 25% of them happening multiple times in a year. The types of attacks are diverse, ranging from human-caused attacks like phishing campaigns and theft, to technical ones like software and malware failure. Interestingly, the results showed that different types of CSOs experience different types of attacks, with CBOs and Local NGOs experiencing the highest rates of attacks compared to international NGOs. However, there was no clear correlation between the level of digital security and how established a CSO is. These findings paint a picture of an urgent need for digital security awareness and preparedness in the region.

This study also provides a comprehensive overview of the exposure of CSOs in West Africa to digital security threats and attacks. It highlights the digital technologies adopted by these organisations, their key activities in terms of digital safety, and their current level of secure digital practices. The results indicate that although emails are the most used digital technology, the majority of CSOs lack proper knowledge and training on how to protect themselves from digital threats and attacks. Additionally, there is a significant gap in the level of digital security practices among CSOs, with many failing to implement basic measures such as updating their operating systems and using virtual private networks. Furthermore, limited financial resources prevent many CSOs from allocating a budget for information security, leaving them vulnerable to digital threats and attacks. These findings highlight the pressing need for CSOs in the region to invest in digital security education and training and to collaborate with government and other organisations to put in place the necessary measures to secure their digital tools and protect themselves from digital security threats and attacks.

In addition, the findings of this study show that CSOs in West Africa are facing a significant gap in their preparedness towards responding to digital security threats and attacks. Most of the few with digital security training experiences are self-taught, implying that individuals do not receive enough training from their employers. The lack of digital security training and understanding of best practices leaves CSOs vulnerable to potential breaches and loss of valuable data. This study highlights the importance of digital security to CSOs and the impact that targeted training programmes can have in improving their overall preparedness. The study presents several insights that can serve as a valuable starting point for creating comprehensive and effective digital security training programmes that can empower West African CSOs to operate securely in the digital space.

The report further highlights the importance of having robust digital security laws and policies in place in West Africa. Despite efforts from many countries, more needs to be done to ensure that individuals and organisations are protected from digital threats and attacks. Remarkably, only six (6) countries in West Africa (Benin, Burkina Faso, Cape Verde, Ghana, Mali and Senegal) have comprehensive data protection laws. Also, the finding that 45% of CSOs are unaware of national laws and regulations on digital security underscores the need for better education and awareness efforts. Additionally, the argument that some countries have weaker privacy regulations to gain a competitive advantage highlights the need for a harmonised approach to digital security laws and policies across West Africa. Yet, with regards to harmonisation of the national digital security policies with other international digital security policies, only Cape Verde, Ghana, Guinea, Niger, Senegal and Togo have digital security policies well harmonised, particularly with the African Union Convention on Cyber Security and Personal Data Protection policy.

The findings in this report further shed light on the reality of the lack of security measures in place within West African CSOs. Despite the increasing reliance on technology and the use of personal and organisational devices, only a small portion of CSOs have a computer and information security policy in place. Furthermore, even among those who have a policy in place, many do not fully understand its contents and have been known to deviate from it. Additionally, the fact that so many individuals are using their devices for both personal and professional use, and the high number of lost devices, highlights the pressing need for stronger security measures and guidelines for digital security within organisations. CSOs in West Africa need to take the necessary steps to ensure the security of their digital assets and protect themselves against potential digital threats.

To end, this study has shown also that West African CSOs are faced with a multitude of digital security challenges that threaten to undermine their efforts in pursuing their mandates. From a lack of financial resources, inadequate ICT and digital security infrastructure to a dearth of digital security training and policies, the situation is dire. CSOs are left vulnerable to fraudsters posing as genuine funders and cyber-attacks that may compromise sensitive information. It is imperative that CSOs take action to address these challenges and enhance their digital security posture. This requires an investment in technology and personnel, as well as the implementation of comprehensive digital security policies and training programmes that can keep pace with the rapidly changing digital security landscape. By doing so, CSOs can continue to pursue their mandates with confidence and help ensure a safer and more secure digital environment for all.

Recommendations

This study contextually integrates several recommendations into the various chapters while presenting and discussing the results. However, based on the findings altogether, the following recommendations can be made:

At the CSO level

1. **Increase Awareness on Digital Security:** This study has shown that digital security awareness level is very low among the CSOs in West Africa. CSOs should be made aware of the digital threats that exist and how these threats can harm their organisations. This could be done through workshops, training sessions, and seminars, where digital security experts can share their knowledge and provide practical tips on how to protect against these threats. WACSI like few other organisations have shown the way through its webinars and workshops on digital security. These efforts should be supported to expand and sustain their reach, and many more organisations should champion this effort, within their networks and communities.

2. **Invest in Digital Security Infrastructure:** It is time for CSOs to cease to be pirates! CSOs who rely on pirated software for their operations need to understand that this software is a direct source of threat to their digital devices and systems. CSOs in West Africa should invest in digital security infrastructure, such as firewalls, antivirus software, and encryption, to protect their digital assets from cyber-attacks. For example, by investing in a good antivirus software, CSOs can prevent malware from infiltrating their systems, which can lead to data breaches.

3. **Develop a Computer and Information Security Policy:** CSOs in West Africa should develop a computer and information security policy that outlines the security measures and protocols that are in place to safeguard digital assets from digital security threats. It should be communicated to all employees

within the organisation to ensure that they understand the contents and their role in maintaining digital security. An example of the contents of such a policy could be to mandate strong password requirements for all accounts, regularly update software and install security patches, prohibit the use of unapproved third-party software or hardware, encrypt sensitive data and implement access controls, and monitor the network for suspicious activity. This policy can serve as a guide to maintaining a secure digital environment and minimising the risks associated with digital security threats.

4. **Train Employees on Digital Security:** The analysis has shown that there is a strong interest among CSOs in West Africa in developing their digital security skills and knowledge. It would therefore be important for CSOs to invest in training their employees on digital security, so that they can identify and respond to potential threats. For example, employees can be trained on how to identify phishing emails, how to securely store passwords, and how to detect and report security incidents. The training should be tailored to the needs of the CSOs focusing on hands-on experience and practical knowledge on the topics they have expressed interest in.
5. **Use Strong Passwords and Authentication Measures:** CSOs should implement strong password policies, such as using a combination of letters, numbers and symbols, and regularly update their passwords. They should also use multi-factor authentication measures, such as biometric identification or SMS verification, to ensure the highest level of security for their digital assets. Some CSOs that have participated in training programmes, including previous WACSI webinars, that taught them how to use strong passwords and 2-factor authentication, attested that these have proved very useful, as some respondents recounted in this study.

6. **Regularly Backup Data:** Regularly backing up data is a crucial step in protecting against data loss, which can occur because of a cyber-attack, theft of ICT devices or other means. CSOs in West Africa should consider implementing a regular backup system to protect their data. For example, this can be done by using cloud storage solutions (such as Dropbox, Google Drive, OneDrive, Box or Amazon Web Service). These cloud-based storage services provide an easy-to-use and cost-effective way to store data remotely, reducing the risk of losing data in case of a cyber-attack or other disasters. With cloud storage, CSOs can set up automatic backups

of their data, which can be accessed from anywhere at any time. This ensures that even if their computers are compromised, the data can still be recovered, and the organisation can continue its operations.

7. **Secure Remote Access:** Secure remote access is a crucial aspect of digital security that should not be overlooked by CSOs. With the increasing trend of remote work, employees sometimes need to access their organisation's systems from remote locations, which exposes the system to various security threats. To address this, CSOs should implement a secure remote access solution such as Virtual Private Networks (VPNs). A VPN can encrypt all data transmitted between the employee's device and the CSO's system, ensuring that sensitive data is not intercepted by unauthorised parties. For example, a CSO that provides legal aid services to vulnerable groups may have employees who work remotely to reach clients in different regions of the country. By implementing a VPN, the CSO can ensure that their employees can securely access their systems and client data from remote locations, without fear of interception by unauthorised parties. The VPN solution will encrypt all data transmitted between the employee's device and the CSO's system, ensuring that sensitive data is kept secure. Also, the VPN can be configured to limit access to only authorised personnel, thus providing an additional layer of security.

8. **Implement Mobile Device Management (MDM):** MDM solutions can help CSOs to secure their digital assets and mobile devices. These solutions can ensure that employees' devices are configured according to the organisation's security policies and that sensitive data is encrypted to prevent unauthorised access. Moreover, MDM can allow for the remote wiping of lost or stolen devices to prevent data breaches. A CSO could for instance, use an MDM solution to keep track of their ICT devices such as smartphones and tablets, ensuring that they are properly configured and updated with the latest security patches. If a device is lost or stolen, the MDM solution could be used to remotely wipe the device and protect sensitive data from falling into the wrong hands. By implementing MDM solutions, CSOs can increase their digital security and protect their digital assets and data.

9. **Monitor Devices:** Monitoring devices is crucial for CSOs to detect and respond to security incidents quickly. By continuously monitoring their

devices, CSOs can detect unusual activity, such as suspicious network traffic or unauthorised access attempts, and take action to prevent potential threats from escalating. As an example, a CSO can use intrusion detection and prevention systems (IDPS) to monitor their network and detect security incidents in real-time. Also, regularly scanning for vulnerabilities can help identify potential weaknesses in the system that could be exploited by attackers. By addressing these vulnerabilities, CSOs can reduce their risk of digital security attacks and protect their sensitive data.

10. **Implement a Disaster Recovery Plan:** Implementing a disaster recovery plan is crucial for CSOs to ensure continuity of their operations and minimise the impact of a digital security attack or other disaster. The plan should outline the steps to take in the event of an attack, such as identifying the source and scope of the attack, containing the attack, and recovering from the damage caused. It should also include protocols for restoring systems and data, and for communicating with stakeholders, such as clients, partners, and employees. One example of this is the use of a cloud-based disaster recovery solution. This solution enables CSOs to back up critical data and applications to a remote, secure location, which can be easily recovered in the event of a disaster or attack. This ensures that they can quickly recover from a security incident and minimise the damage to their operations and reputation.

11. **Regularly Update Software:** CSOs in West Africa should regularly update their software, including operating systems, applications, and security software, to ensure that they are protected against known vulnerabilities. For instance, if an organisation fails to update its security software, it may be vulnerable to a new type of malware that exploits a known vulnerability. This can result in data loss, financial loss, and reputational damage. Therefore, CSOs should implement a regular software update policy to ensure that all software is up to date. This can be achieved by using automated software update tools, such as Windows Update, which automatically downloads and installs the latest security patches and updates. In addition, CSOs can, through their ICT policies, mandate employees to update software promptly when required.

12. **Appoint Cybersecurity Leader:** CSOs should appoint a cybersecurity leader who can oversee their digital security efforts, identify potential threats and respond to incidents in

a timely manner. This person should be trained and have the necessary resources to effectively manage the organisation's digital security. A practical example of this is a CSO based in Ghana that appointed a cybersecurity leader to manage its digital security. The leader worked closely with the organisation's IT team to develop and implement digital security policies and procedures. They also conduct regular training sessions for staff members to ensure that everyone is aware of the organisation's digital security protocols. The cybersecurity leader is responsible for monitoring the organisation's digital systems for any suspicious activities and responding to any incidents in a timely manner. This appointment has resulted in the organisation's digital security being strengthened, and its staff members being more vigilant and aware of potential digital security threats.

13. **Consider outsourcing digital security services:** Outsourcing digital security services can be a cost-effective solution for CSOs to address their digital security needs. By outsourcing to specialised companies, CSOs can access expert skills and knowledge that may not be available in-house, and ensure that their digital security measures are up-to-date and effective. This can be especially beneficial for CSOs that may not have the resources to invest in building an in-house digital security team or acquiring the necessary tools and technologies. Additionally, outsourcing can provide a level of objectivity and independence in evaluating digital security risks and identifying vulnerabilities. However, CSOs should carefully evaluate potential service providers and ensure that they have a strong track record of delivering quality services and protecting client data.

14. **Collaborate with relevant stakeholders:** By collaborating with government agencies, private sector companies, and other CSOs, CSOs can share information and resources on digital security best practices, and collectively pool efforts in preventing and responding to digital security threats. This collaboration will help to promote a culture of digital security awareness and enhance the capacity of CSOs to address digital security threats effectively. Additionally, CSOs can leverage the knowledge and expertise of relevant stakeholders in developing digital security policies and strategies that are appropriate for their unique needs and context. Ultimately, collaboration with relevant stakeholders can help CSOs to better protect their digital assets and ensure the continuity of their operations.

15. **Regularly review and update security practices:** As the digital landscape is constantly evolving, the risks and threats facing organisations also change. This means that CSOs must be proactive in their approach to digital security and stay informed about the latest threats and risks. Encouraging CSOs to regularly review and update their digital security practices will help ensure that they are well equipped to respond to evolving risks and threats. This can involve regularly conducting security audits, using software and tools to monitor their digital systems, and updating their digital security policies and procedures. In addition, CSOs should invest in regular digital security training for their staff and volunteers to update or build their awareness and understanding of the importance of digital security. By regularly reviewing and updating their digital security practices, CSOs in West Africa will be better positioned to protect themselves and their stakeholders from digital security threats and risks.

At the national level

Despite the largely restrictive civic space in West Africa, with many governments imposing various forms of limitations on the activities of civil society both online and offline, it is critical that governments prioritise the digital security of CSOs. The ability of CSOs to operate freely and communicate securely with their stakeholders is a fundamental tenet of any functioning democracy (Nanz and Steffek, 2017). Digital security breaches among CSOs can have far-reaching implications beyond just the CSO because they often handle sensitive information about individuals and communities. For instance, if a CSO holds confidential information about individuals or groups that are exposed, it can put those individuals or groups at risk of identity theft, fraud, harassment, violence, and other malicious activities. Governments have a responsibility to protect their citizens, and supporting CSOs' digital security efforts should be seen as a vital component of this responsibility. Supporting CSOs' digital security efforts helps to ensure not only a robust and dynamic civil society, but also a more open and transparent democratic society and a safe environment for everyone. The following five (5) recommendations outlined are, therefore, crucial steps towards achieving this goal, even if they may seem unlikely to be fully implemented in the current restrictive civic space.

1. **Develop and implement comprehensive national level policies on digital security:** Governments in West Africa should work with experts in the field of digital security to develop and implement policies that take into consideration the rapidly changing digital landscape (Dlamini, Taute and

Radebe, 2011). These policies should address issues such as data protection, the responsibilities of service providers, the reporting of and response to digital security incidents and the protection of individuals' personal information.

2. **Support the capacity building of CSOs:** Governments in West Africa should support the capacity building of CSOs and communities to enhance their ability to safeguard themselves against digital security threats and attacks. This can include providing training in digital security best practices, technical assistance, and funding for digital security infrastructure. For instance, Calandro and Berglund (2019) found that in Southern Africa, public education or training programs on digital security are typically led by the government agency responsible for cybersecurity. Particularly, in Zimbabwe, the Ministry of ICT launched an annual Cybersecurity Awareness Week, while South Africa's Cybersecurity HUB has public awareness and safety campaigns, and Mauritius' National Computer Board offers cyber capacity and safety training for individuals and businesses. In Ghana, the Ministry of Communication and Digitalisation recently launched the National Cyber Security Awareness Month (NCSAM)[10] 2022, under the theme "Regulating Cybersecurity: A Public-Private Sector Collaborative Approach," and the Cyber Security Authority (CSA) is promoting cybersecurity awareness through radio ads. Other West African countries can follow Ghana's example and promote similar initiatives to strengthen digital security capacity building.

3. **Encourage the development of a strong cybersecurity culture within CSOs:** Governments should facilitate a proactive approach to digital security among CSOs, encouraging the establishment and review of best practices and policies. Funding for digital security assessments, incentives for implementation, and sharing of best practices and lessons learned should also be promoted. Kechagias et al. (2022) argue that digital security threats are a matter of national security and should be managed as such, and Scully (2014) emphasises the importance of government support for digital security efforts in democratic societies.

4. **Foster partnerships among CSOs, the private sector and state actors:** Governments in West Africa are encouraged to promote partnerships among civil society organisations (CSOs), private sector, and state actors to facilitate the exchange of cutting-edge digital security technologies and resources and promote cybersecurity awareness (Scully, 2014). To achieve this, governments can provide funding

[10] See National Cyber Security Awareness Month (NCSAM). (n.d.). Retrieved January 25, 2023, from https://ncsam.csa.gov.gh/

for digital security collaboration initiatives and encourage sharing of digital security information and best practices. Nugraha and Putri (2016) highlight the significance of coordination among government agencies and various stakeholders, including private sector and civil society, for cybersecurity awareness using the example of Indonesia. They illustrate how the Coordinating Ministry of Politics, Law, and Security in Indonesia initiated a Cybersecurity Forum, an informal group consisting of a range of cybercrime actors such as business representatives, police departments, and CSOs to discuss cyber attack and governance issues (ibid).

5. **Strengthen the legal framework for digital security:** Governments in West Africa should work to strengthen the legal framework for digital security, including measures to prevent and respond to digital attacks, and to protect the privacy and security of CSOs' sensitive information. Governments must ensure that the laws and regulations surrounding digital security are implemented and enforced (Dlamini et al., 2011; Odumesi, 2014). This can include regular inspections and audits of digital security practices, ensuring that CSOs are aware of their legal obligations, and enforcing penalties for non-compliance with digital security laws and regulations. Governments must also work with international institutions to ensure that international digital security standards are being met.

Conclusively, CSOs in West Africa face significant challenges in ensuring their digital security, but by implementing these recommendations, and with the support of government, they can reduce their risk of falling victim to digital security threats and better protect their assets, data, and information. Also, by collaborating with relevant stakeholders, they can help to create a safer digital environment for all West Africans.

BIBLIOGRAPHY

Access (2014). One of these things is not like the other: A report on fake domain attacks. Retrieved from: https://s3.amazonaws.com/access.3cdn.net/a80a7cabdf0d-dadc85_vdm6brria.pdf p.8 (Accessed 30 December, 2022).

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index. SSRN Electronic Journal, 1–21. https://doi.org/10.2139/ssrn.3142296.

African Union (2023). List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection of 2014. https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf (Accessed: 24 February, 2023).

African Union Commission and Symantec (2016) "Cyber crime and cyber security trends in Africa," Global Forum for Cybersecurity Expertise Initiative, Addis Ababa, Ethiopia, techreport, Oct. Retrieved from: https://www.thegfce.com/binaries/gfce/documents/publications/2017/03/10/report-cyber-trends-in-africa/ Cyber+security+trends+report+Africa-en.pdf (Accessed 30 November, 2022).

Aikins, M. (2012.) 'The spy who came in from the code.' Columbia Journalism Review. Retrieved from: http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all (Accessed 22 December, 2022).

Anderson, R. (2001, December). Why information security is hard-an economic perspective. In Seventeenth Annual Computer Security Applications Conference (pp. 358-365). IEEE.

Anheier, H. K., Lang, M., & Toepler, S. (2019). Civil society in times of change: shrinking, changing and expanding spaces and the need for new regulatory approaches. Economics, 13(1).

Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in Africa: an empirical study. Proceedings of the 8th International Conference on Cyber Warfare and Security (pp. 78-83). Retrieved from https://www.thinkmind.org/index.php?view=instance&instance=CYBER+2018 doi:10.17863/CAM.40856

Badio, H. and Dillon, E. (2017). Cybercrime- Challenges Faced By Liberia September 11, 2017.

Calandro, E., & Berglund, N. (2019). Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case. In GIGAnet annual symposium. Berlin. https://researchictafrica. net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1. pdf. (Accessed 20 February, 2023).

CIPESA. (2019). Digital Rights in The Gambia Submission to the 34th session of the Universal Periodic Review, The Gambia, 2019.

Citizen Lab. (2013.) 'Monitoring Information Controls During the Bali IGF.' Retrieved from: https://citizenlab.org/2013/10/monitoring-information-controls-bali-igf/ (Accessed 21 November, 2022).

CIVICUS. (2022). State of Civil Society Report 2022. Retrieved from https://www.civicus.org/documents/reports-and-publications/SOCS/2022/CIVICUS2022SOCSReport.pdf (Accessed 28 February, 2023).

CIVICUS. (2018). State of Civil Society Report 2018. Year in Review: Top Ten Trends. Retrieved from https://www.civicus.org/documents/reports-and-publications/SOCS/2018/socs-2018-overview_top-ten-trends.pdf (Accessed 9 February, 2023).

Cogburn, D. L. (2004). Diversity matters, even at a distance: Evaluating the impact of computer-mediated communication on civil society participation in the World Summit on the Information Society. Information Technologies & International Development, 1(3), pp-15.

Committee to Protect Journalists. (2014) 1046 Journalists Killed since 1992. Committee to Protect Journalists. https://www.cpj.org/killed/. (Accessed 19 December 2022) According to CPJ's methodology, 'threatened journalists' includes 'all forms of threats at any time before a journalist was murdered.'

Cooper, R. (2018). What is civil society? How is the term used and what is seen to be its role and value (internationally) in 2018. K4D Helpdesk Report, Brighton, UK: Institute of Development Studies. (Accessed 20 November, 2022).

Crete-Nishihata, M., Dalek J., Deibert R., Hardy, S., Kleemola, K., McKune, S., Poetranto, I, Scott-Railton, J., Senft, A., Sonne, B., and Wiseman, G. 'Communities at Risk: Targeted Digital Threats Against Civil Society'. Citizen Lab, 11 November 2014. Retrieved from: https://targetedthreats.net/.https://targetedthreats.net/media/1-ExecutiveSummary.pdf (Accessed 21 November, 2022).

Crete-Nishihata, M., Dalek, J., Maynier, E., & Scott-Railton, J. (2018). Spying on a budget: Inside a phishing operation with targets in the tibetan community. The Citizen Lab. Retrieved from https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/ (Accessed 21 November, 2022).

Daigle, B. (2021). Data protection laws in Africa: A pan-African survey and noted trends. J. Int'l Com. & Econ., 1.

Dataguidance (2017). Mauritania. Retrieved from: https://www.dataguidance.com/jurisdiction/mauritania (Accessed on 20 December, 2022).

Dlamini, I. Z., Taute, B., & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. Proceedings of Southern African Cyber Security Awareness

Workshop (SACSAW) 2011. Retrieved from https://researchspace.csir.co.za/dspace/bitstream/handle/10204/5163/Dlamini_2011.pdf?sequence=1 (Accessed 20 February, 2023).

Dutton, W. H. (2011). Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet. Report for UNESCO's Division for Freedom of Expression, Democracy and Peace. Retrieved from Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet - UNESCO Digital Library (Accessed 9 February, 2023).

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109.

Fighting Cybercrime in Nigeria (2011) (Fighting Cybercrime in Nigeria, www.thorpepodcast.wordpr ess.com.2011).

Fisher, D. (2013.) 'What is a Man-in-the-Middle Attack?' Kaspersky Lab Daily. http://blog. kaspersky.com/man-in-the-middle-attack/ (Accessed 3 December, 2022).

Florini, A. M. (Ed.). (2012). The third force: The rise of transnational civil society. Brookings Institution Press.

Freedom House. (2014). Freedom on the net report. Venezuelan Chapter. Disponible en línea: https://freedomhouse. org/report/freedom-net/2014/venezuela Consultado el, 18(03), 2018.

Friedersdorf, C. (2014). Eyes over Compton: How police spied on a whole city. The Atlantic. Retrieved from: http://www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/ (Accessed 21 November, 2022).

Galperin, E., & Marquis-Boire, M. (2012). Syrian Activists Targets with Facebook Phishing Attack. Electronic Frontier Foundation.

GDPR (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing directive 95/46. Official Journal of the European Union (03) 59:1-88

Government of Ghana (2021) Cybersecurity Act, 2020, Act 1038. Ghana Publishing Company Ltd. Assembly Press, Accra.

Habermas, J. (1991). The Structural Transformation of the Public Sphere, Cambridge, MA: MIT Press.

Hulcoop, A., Brooks, M., Maynier, E., Scott-Railton, J.,& Crete-Nishihata, M. (2016). It's parliamentary: KeyBoy and the targeting of the Tibetan community. Retrieved from https://citizenlab.ca/2016/11/parliament-keyboy/ (Accessed 21 November, 2022).

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.

Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). Building digital safety for journalism: A survey of selected issues. UNESCO Publishing.

Hess, A. (2014.) 'Why Women Aren't Welcome on the Internet.' Pacific Standard. http://www.psmag.com/navigation/health-and-behavior/women-arent-welcome-internet-72170/(Accessed 14 November, 2022).

International Centre for Missing & Exploited Children (ICMEC) (2010). Child Pornography: Model legislation and Global review, 6th edn, Koons Family Institute on International Law and Policy. Retrieved from http://icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf (Accessed on 29 December, 2022).

International Criminal Police Organisation (INTERPOL) (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-showsalarming-rate-of-cyberattacks-during-COVID-19.

International News Safety Institute (2014). Journalism Safety: Threats to Media Workers and Measures to Protect Them. INSI. Retrieved from: http://www.newssafety.org/latest/news/insi-news/detail/insi-publishes-good-practice-safety-guide-for-journalists-and-media-workers-1354/ (Accessed 12 December, 2022).

International News Safety Institute and International Women's Media Foundation (2014). Violence and Harassment Against Women in the News Media: A Global Picture. Retrieved from: http://www.iwmf.org/executive-summary/ (Accessed 2 December, 2022).

Jagalur, P. K., Levin, P. L., Brittain, K., Dubinsky, M., Landau-Jagalur, K., & Lathrop, C. (2018). Cybersecurity for civil society. In 2018 IEEE International Symposium on Technology and Society (ISTAS) (pp. 102-107). IEEE.

Kalemera, A., Kapiyo, V., Paul, K., Nalwoga, L., Nanfuka, J., Wanyama, E., and Wakabi, W., (2020). "State of internet freedom in Chad 2019: Mapping trends in government internet controls, 1999–2019". CIPESA. January 2020. https://cipesa.org/?wpfb_dl=323.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.

Lucchetti, M. (2018) 'Cybercrime Legislation in Africa: Regional and International Standard' (GLACY+-Global Action on Cybercrime Extended) 12 April 2018 <https://au.1nt>newsevents> (Accessed 17 November, 2022).

Lynn, T., Rosati, P., Conway, E., Curran, D., Fox, G., & O'Gorman, C. (2022). Digital Technologies and Civil Society. In Digital Towns: Accelerating and Measuring the Digital Transformation of Rural Societies and Economies (pp. 91-108). Cham: Springer International Publishing.

Makeri, Y. A. (2017). Cyber security issues in Nigeria and challenges. International Journal, 7(4).

McDowell, M. (2013.) Security Tip (ST04-015) Understanding Denial-of-Service Attacks. United States Computer Emergency Readiness Team. Retrieved from: https://www.us-cert.gov/ncas/tips/ST04-015 (Accessed 29 December 2022).

Nanz, P., & Steffek, J. (2017). Deliberation and democracy in global governance: The role of civil society. In Participation for Sustainability in Trade (pp. 61-72). Routledge.

Nugraha, L. K., & Putri, D. A. (2016). Mapping the cyber policy landscape: Indonesia. Global Partners Digital, 1-28.

Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. Computer Science and Engineering, 2(6), 98-100.

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116-125.

Piper, D. L. A. (2023). DLA Piper global data protection laws of the world-World Map. Data Protection Laws of the World, Chad. Retrieved from https://www.dlapiperdataprotection.com

PWC. (2021). Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne. Rapport d'enquête sur la cybersécurité.

Rich, C. (2016) Privacy Laws in Africa and the Near East (16) 6 Bloomberg BNA World Data Protection Report, 1.

Rights Con 2014. (2014.) Panel Session. 'Watching the Observers: The Impact of Surveillance on Human Rights.' Retrieved from: https://www.youtube.com/watch?v=rbqHyNt-j9XU&list=PLprTandRM9601CNiM-d4VVTglZ1YSglKGx (Accessed 30 December, 2022).

Rydzak, J., Karanja, M., & Opiyo, N. (2020). Internet Shutdowns in Africa| Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries. International Journal of Communication, 14, 24.

Scholte, J. A. (2002). Civil society and democracy in global governance. Global governance, 8(3), 281-304.

Scully, T. (2014). The cyber security threat stops in the boardroom. Journal of business continuity & emergency planning, 7(2), 138-148.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

The Indian Law Institute (2010). Introduction to the cyber world and cyber-Law.

Toussi, S. (2020). New Mali cybercrime law potentially problematic to digital rights. CIPESA. February 21, 2020. Retrieved from: https://cipesa.org/2020/02/new-mali-cyber-crime-law-potentiallyproblematic-to-digital-rights/ (Accessed on 29 December, 2022).

Toussi, S., & Robertson, T. (2020, August 10). Niger passes new law on interception of communications. CIPESA: ICT Policy Centre for Eastern and Southern Africa. Retrieved from https://cipesa.org/2020/08/niger-passes-new-law-on-interception-of-communications/ (Accessed 21 January, 2023).

Turianski, Y. (2018). 'Balancing Cyber Security and Internet Freedom in Africa', SAIIA Occasional Paper, 275, 2018, http://www.saiia.org.za/occasional-papers/1292-balancingcyber-security-and-internet-freedom-in-africa/file (Accessed 9 February, 2023).

UNCTAD (2015). Review of E-Commerce Regulation Harmonisation in the Economic Community of West African Countries. Geneva: UNCTAD

UNESCO (2012). 'UN Plan of Action on the Safety of Journalists and the Issue of Impunity.' Retrieved from: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/UN_plan_on_Safety_Journalists_EN.pdf (Accessed 15 December 2022.)

United Nations Institute for Disarmament Research (UNIDIR) (2019). Cyber Policy Portal, Mauritania. Retrieved at: https://cyberpolicyportal.org/states/mauritania (Accessed on 20 December, 2022).

Wafa, T. (2009). 'Global Internet privacy rights – a pragmatic approach', University of San Francisco Intellectual Property Law Bulletin, 13 (131).

World Bank Group. (2016). World development report 2016: Digital dividends. World Bank Publications.

APPENDICES

Appendix 1

Descriptive statistics of survey respondents

Table A 1: Descriptive statistics of survey respondents

	Freq. (N)	Percentage	Cum.
Gender of respondent			
Male	194	69.29	69.29
Female	85	30.36	99.64
Prefer not to say	1	0.36	100
Position/job level			
Entry level	14	5.13	5.13
Intermediate or experienced level	44	16.12	21.25
First level management	24	8.79	30.04
Middle-level management	41	15.02	45.05
Senior executive/top level management &	150	54.95	100
Education of respondent			
Secondary school	6	2.14	2.14
Post graduate	115	41.07	43.21
Tertiary /university/graduate	159	56.79	100
Respondents by country			
Benin	24	8.6	8.6
Burkina Faso	8	2.87	11.47
Cameroon	7	2.51	13.98
Chad	8	2.87	16.85
Côte d'Ivoire	19	6.81	23.66
The Gambia	4	1.43	25.09
Ghana	58	20.79	45.88
Guinea	14	5.02	50.9
Guinea-Bissau	1	0.36	51.25
Liberia	3	1.08	52.33
Mali	9	3.23	55.56
Mauritania	1	0.36	55.91
Niger	12	4.3	60.22
Nigeria	91	32.62	92.83
Senegal	4	1.43	94.27

Sierra Leone	9	3.23	97.49
Togo	7	2.51	100
Type of CSO			
Community-Based Org. (CBO)	48	17.39	17.39
International Non-Governmental Org. (INGO)	28	10.14	27.54
Local Non-Governmental Org. (LNGO)	106	38.41	65.94
Other Organisations	94	34.06	100
CSOs by activity			
Politics and Governance	16	5.73	5.73
Conflict, Peace and/or Security	35	12.54	18.28
Accidents and Disasters	2	0.72	19
Human Rights (incl. women, children, mi	153	54.84	73.84
Health and sanitation	3	1.08	74.91
Education	24	8.6	83.51
Technology and Innovation	3	1.08	84.59
Religion and Culture	2	0.72	85.3
Poverty and hunger	14	5.02	90.32
Environment, climate change & sustainability	10	3.58	93.91
Other	17	6.09	100

Source: WASCSI (2023)

Description of Key Informant Interviewees

Table A 2: Description of Key Informant Interviewees

ID	Gender	Education[a]	Position	country	CSO classification[b]	CSO type
KII1	Male	Post graduate	Executive Director	Nigeria	Human Rights	CBO
KII2	Male	Tertiary	Executive Director	Togo	Human Rights	INGO
KII3	Male	Tertiary	Project Coordinator	Ghana	Conflict, Peace and/or Security	CBO
KII4	Male	Tertiary	Executive Director	Ghana	Human Rights	CBO
KII5	Male	Post graduate	Executive Director	Benin	Human Rights	LNGO
KII6	Male	Tertiary	Executive Director	Côte d'Ivoire	Human Rights	INGO
KII7	Male	Tertiary	Executive Director	Guinea	Human Rights	INGO
KII8	Male	Tertiary	President	Cameroon	Education	Other
KI9	Male	Tertiary	Project Manager	Niger	Human Rights	Other
KII10	Female	Post graduate	Executive Director	Guinea-Bissau	Human Rights	LNGO
KII11	Male	Tertiary	Executive Director	Liberia	Conflict, Peace and/or Security	CBO

KII12	Female	Post graduate	Head of Media and Communications	Nigeria	Other	LNGO
KII13	Male	Tertiary	Finance and Administrative Manager	Ghana	Human Rights	LNGO
KII14	Male	Post graduate	MEL Officer	Nigeria	Human Rights	LNGO
KII15	Male	Post graduate	Executive Director	Nigeria	Politics and Governance	LNGO
KII16	Male	Tertiary	Chief of Operations	Nigeria	Conflict, Peace and/or Security	LNGO
KII17	Male	Tertiary	Executive Director	Nigeria	Poverty and hunger	Other
KII18	Male	Tertiary	Executive Director	Ghana	Human Rights	CBO
KII19	Male	Post graduate	Director of programs	Nigeria	Conflict, Peace and/or Security	LNGO
KII20	Male	Tertiary	Media and Communication Officer	Nigeria	Other	LNGO
KII21	Male	Tertiary	Care and support officer	Nigeria	Human Rights	CBO
KII22	Male	Tertiary	Monitoring and Evaluation Officer	Nigeria	Conflict, Peace and/or Security	CBO
KII23	Male	Post graduate	Cadre	Côte d'Ivoire	Human Rights	Other
KII24	Male	Tertiary	Chairman, Board of Directors	Liberia	Human Rights	LNGO

Note: [a]"Tertiary" implies completed university education but not post graduate.
[b]"Human Rights" includes organisations protecting the rights of women, children, and minorities.

Source: WACSI (2023)

Table A 3: Cost Estimation of Device Theft/Loss

	Nigeria			Ghana			Liberia			Côte d'Ivoire		
	Qty	Unit	Total	Qty	Unit	Total	Qty	Unit	Total	Qty	Unit	Total
PC (Desktops)	5	600	2999.95	1	599.99	599.99	0	599.99	0	3	599.99	1799.97
Laptops	15	390	5849.85	11	389.99	4289.89	9	389.99	3509.91	5	389.99	1949.95
Tablets/Air pads	4	230	919.96	0	229.99	0	0	229.99	0	1	229.99	229.99
Mobile Devices	5	120	599.95	8	119.99	959.92	5	119.99	599.95	5	119.99	599.95
Storage Devices	4	51.99	207.96	2	51.99	103.98	3	51.99	155.97	2	51.99	103.98
Network Devices	1	80.99	80.99	2	80.99	161.98	1	80.99	80.99	1	80.99	80.99
	Total		10,658.66	Total		6,115.76	Total		4,346.82	Total		4,764.83
Average: 6,471.52												

Table A 4: Cost Estimation of Data Loss

Cost Item	Ghana	Nigeria	Liberia	Niger	Guinea-Bissau	Côte d'Ivoire
Number of records	2,000	4,000	1,000	1,000	1,200	1,500
Incident Investigation	177,800	178,600	177,400	177,400	177,480	177,600
Client Notification / Crisis Management	39,650	49,300	34,825	34,825	35,790	37,238
Regulatory Fines & Penalties	58,700	117,400	29,350	29,350	35,220	44,025
Personal card information (PCI)	-	-	-	-	-	-
Class Action Lawsuit	324,000	326,000	323,000	323,000	323,200	323,500
Total Cost	600,150	671,300	564,575	564,575	571,690	582,363
Average: $ 592,442						

Interviews used:

Nigeria – KII20, KII5, KII17, KII12
Ghana – KII3, KII8
Liberia – KII24
Côte d'Ivoire – KII9
Niger – KII9

Guinea-Bissau – KII10

Additional notes on study methodology

Study limitations:

As in any research, this study faced some limitations. First, the survey was disseminated to a prepared list of sample CSOs in West Africa, which means that it does not represent a random sample of the population since the list of the population was not exhaustive. Secondly, the response rate may have been influenced by the number of inactive CSOs on the sample frame, fear of participating in online surveys, technical digital terminologies, survey fatigue, and the length of the survey, especially for key informant interviews. To address these likely concerns, the study structured the survey into sizable sections to make it easy to navigate, shortened the length of the questionnaire, assured respondents of confidentiality and anonymity of responses, and simplified technical jargons. Additionally, the study used phone calls to reach CSOs that were difficult to reach through emails, but some countries like Cape Verde were least reached due to network and technical challenges.

While the lack of cross-country representativeness of the data presented some limitations, particularly regarding the external validity, combining different sources of evidence, such as survey data, desk reviews, and anecdotal evidence through key informant interviews helped to substantiate the external validity of the study, in addition to the internal validity to the sample studied.

Ethical considerations:

The study obtained documented informed consent from the respondents before data collection could start. Participants were not offered any monetary compensation for participating in the study. They were made aware that participation in the study was voluntary, and they could opt-out at any time without consequences. To ensure confidentiality, data was stored securely, and access was granted only to the research team. To ensure anonymity, the collection of personalised data was minimised as much as possible, and no personal information was analysed or reported. These measures ensured that the study was conducted in an ethical manner and protected the rights and privacy of the participants.

Appendix 2

Case Studies Cited in Chapter Two (2)

Box 2. 2: A Malicious Insider Attack

CASE STUDY

This case is based on the experiences of a CSO based in Ghana that focus on advocacy and human rights of minority groups. We interviewed a key informant who shared with us a malicious insider attack they experienced. The attacker, an employee who was let go from the organisation, used their knowledge of the organisation's social media handles and email accounts to gain unauthorised access. The key Informant recounted,

In November of last year, we employed someone who did not meet our standards and was subsequently let go. This individual had access to our social media handles and the email account used to open them, and he was in charge of those social media accounts. After he left, he changed the email addresses associated with those accounts to his personal email address. So eventually, we had official accounts on Facebook, Twitter, and Instagram, but they were linked to someone's personal email. I noticed this and had to reset the emails and passwords. Since the original email was from our organisation, I had access to the passwords, so I was able to change the passwords and remove his email from the accounts. This attack came from an internal individual who was fired but still chose to attack us.

The narrated case reflects an unauthorised access to the organisation's social media accounts by a former employee. The employee, who was responsible for managing the social media accounts, changed the email associated with the accounts to his personal email after he was let go from the organisation. This enabled him to retain control of the accounts, even though he was no longer an employee.

The implications of this experience are significant. The organisation lost control of their social media accounts and the former employee could potentially use them to harm the organisation's reputation or spread false information. In this case, the CSO was fortunate to have identified the attack soon enough to recover the accounts and prevent the attacker from causing serious damage. This highlights the importance of having clear policies in place for handling social media accounts and digital assets in the event that an employee leaves the organisation.

Other CSOs can learn from this experience by ensuring that they have strict access control policies in place for digital assets, such as social media accounts. This could include regularly reviewing and updating who has access to the accounts, having more than one person with relevant access to the accounts, and having procedures in place for removing access when an employee leaves the organisation. Additionally, CSOs should ensure that they have backup copies of login information for digital assets, in case of emergency.
Source of excerpt: KII4

Box 2. 3: Human Error

CASE STUDY

The case could be regarded as a typical example of spam, human error and virus attack. It involves a CSO in Ghana focusing on gender and advocacy, and working to mitigate rural poverty through skill development and training. The organisation has been in operation for a long time and their activities include working on gender community development, gender-based violence, child marriages, teen age pregnancies, environment, food security, and governance and peace. The digital security experienced by the organisation is an issue of spam emails, which are often ignored or deleted. However, there was an instance where the informant received a spam email asking to confirm a receipt and opened it, which led to other spam emails being sent directly to the inbox instead of being marked as spam. The informant also mentioned that members of the organisation sometimes visits websites that are not secured, and inputs their office information, which could be a potential security threat.

We have been operating as an NGO for a long time, and our focus is on gender and advocacy, specifically on mitigating rural poverty through skill development and training. We work to empower women and children through gender community development, gender-based violence prevention, addressing child marriages and teenage pregnancies, and working on environmental, food security, governance, and peace issues.

Recently, we have experienced some digital security issues. We receive a lot of spam emails, which we typically ignore or delete when they end up in the spam folder. However, I recently received an email that appeared to be asking me to confirm a receipt, but when I opened it, there was no receipt. This email was in my spam folder, but then the same email showed up in my inbox the next day. I suspect that opening the email in the spam folder may have given the attacker access to send the same email to my inbox. Additionally, we sometimes visit websites that are not secured to search for proposals and information to update our projects, which can put us at risk for digital security threats or virus attacks. We do not currently back up our activities, which makes us vulnerable to losing important information if we are attacked. As a result, I believe that these issues pose a threat to our organisation going forward, and we need to take steps to better protect ourselves and our data. The organisation also experienced an issue with data loss, as the informant's computer was infected with viruses, and a lot of information was lost. The informant had to copy information to a pen drive and transfer it to a different device to print it, but when the pen drive was inserted into the different device, a threat was detected and the information was deleted. The pen drive is no longer working, and the files that were copied to it are now empty. The information that was lost had to be re-collected, and the organisation had to spend more money to download the information again. The situation also made the informant uncomfortable and unable to report it to their boss.

Last week, I lost a lot of information from my computer to many viruses. I copied the data to a pen drive to a different machine to print, and unfortunately, when I inserted the drive, a threat was detected. In the process of trying to deal with the threat, not knowing, the whole information was deleted; so I had to go back to the original to copy in the evening. Currently, the pen drive I used is no longer working; even if I copy information, the drive will be empty. I can copy information to the drive, but when you copy it to a different machine and open it, it will be empty. I have copied many files and formatted the machine, thinking that I had saved them.

Unfortunately, those files are empty files, and when I open them, I don't see anything. The missing information means that we have to restart again to get the information, which will not be the same as the original. It affected the organisation, and we had to spend more money buying data to download the files hat I had sent through email. Additionally, it made me, the person managing the information, uncomfortable. I couldn't even have reported it to my boss of what happened, so I had to find a way to cover up. As of now, I have most of the files, but they are empty files.

CSOs in West Africa need to be more cautious when visiting websites that are not secured and inputting their official information. Also, as mentioned repeatedly, they need to have proper data backup and virus protection in place to prevent data loss. This case also highlights the importance of having a clear and transparent reporting structure within the organisation, so that issues like this can be reported and addressed quickly.

Source of excerpt: KII13

Box 2. 4: The Reputation Ransom - An NGO's Hacking Hassle

CASE STUDY

This case study is about an NGO Nigeria, where the key informant discusses a digital security issue, they experienced with their social media handle being hacked. The hacker posted inappropriate content on their social media page, damaging the organisation's reputation and integrity. It appears the organisation experiencing issues with their website, which is controlled by a third party and the informant suspects will one day be unexpectedly shut down.

I work with an organisation that focuses on governance, security, health, and education in Nigeria, among other thematic areas such as issues around SDGs. Our social media handles were hacked, and someone posted content unrelated to the organisation's mission. The hacker had access to our social media handles, and people who followed us regularly started asking questions about the content posted. The content was not related to our organisation and contained inappropriate images, such as naked pictures of women, which greatly affected our integrity. We received negative feedback from people who were offended by the images. It was a big blow to our reputation, and it's going to take more effort to control the damage caused. Our website is also another issue, as it's being controlled by a third party, and we have concerns about the safety of the domain. We pay for the domain, and once we pay, they manage most of our things, so the safety of that domain is vital. We are worried that one day it may suddenly be shut down, as we don't have full control over it.

Due to the attack, the NGO's reputation and integrity have been damaged, and they are now in damage control mode trying to explain to their followers that their account was hacked and that the inappropriate content did not come from them. They are also dealing with questions about their credibility and trustworthiness. Apart from the need to secure digital accounts with for e.g.; strong passwords and two-factor authentication, CSOs should be cautious when working with third-party websites or service providers and ensure they have proper security measures in place to protect their online presence and data.

Source of excerpt: KII19

Box 2. 5: A Phishing Attack

CASE STUDY

The following case highlights the experience of a women-care organisation based in Ghana that focuses on advancing the rights of women and transforming the socioeconomic life of rural women entrepreneurs, girls and vulnerable people. They engage in skills development, women rights advocacy, education and health. A Key informant from the CSO recounting a digital security attack experienced in their organisation, narrated as follows.

We received an email from a partner organisation, and because we have a close relationship with them, the content of the email seemed sensitive. I had spoken to the person in the morning, so I thought this colleague would call if it was that urgent. I called back, and we realised that the email was not from him. It seemed like someone had hacked their email system and sent those emails asking for help from other brother organisations.

Clearly, this is a phishing attack. The attacker sent an email that appears to be from a legitimate source in order to trick the recipient into providing sensitive information or clicking on a malicious link. In this case, the attacker used a compromised email account from a partner organisation to send the phishing email to the CSO. Luckily, the recipient realising that the information being request is too sensitive, reached out to the partner organisation by phone call to confirm if the email was indeed from them. The partner organisation then learned that their digital security system has been bridged immediately had to reach out to CSOs that may have received similar emails to alert them of the situation.

It is also interesting to note that apart from receiving phishing emails, the CSO in question also suffered a similar attack where the organisation's Facebook account was hacked and used to send emails to partner organisations, as the key informant added,

We have also experienced our Facebook account being hijacked and used to send mails to our partners. It really affected us because the attackers were asking for money, and it hurt our relationship with our colleagues and partners. When such mails go out, it affects our image. We had to repair our reputation, which took us a month or two of sending mails, making calls, and having meetings to let them know that the messages were not from our organisation.

When asked about how their organisation detected the attack, the key informant responded,

We realised that our email had been hacked when a partner called us about an email they received asking for money from our executive director. We quickly sent out emails from a different address to let our partners know that any messages from the hacked account were not from our organisation. We also made phone calls to partners and contacts we usually communicate with by email to inform them of the situation.

The implication of a phishing attack could be grave. In this particular case, the CSO lost sensitive information, suffered reputational damage and lost a partner. It also led to operational disruption as the key informant continued,

The impact of the attack was that we had to spend time correcting the damage done. It affected our productivity because we had to put our work on hold and go talk to our partners to let them know that any *suspicious mail was not from us. The attack caused delays in our work and some people even belittled us for not being prepared. It damaged the image of our organisation, and we had to do a lot of damage control to repair it. All this takes away from the time we have to do good work, and instead, we have to spend time correcting mistakes. When asked whether they lost a partner in consequence, the respondent confirmed, Yes, there are some partners that are not in good terms with us because they have since then asked us to do a few things. I think one partner is not corresponding very well, so yes, we lost one partner.*

Following this experience, the CSO sought the services of an external colleague to help them learn how to operate safely in the digital space as the respondent went on to share.

Honestly, it helped us to learn so many things about how the digital system works now. We called in someone to come and do some briefing and also tell us how to operate when it comes to the social media aspect. So that is it.

This case highlights the importance of being cautious when receiving emails from unknown or unexpected sources and verifying the authenticity of the sender before responding or clicking on any links. It also shows that even when the sender is known, it might be useful to use other media to cross-check or verify whether the email is indeed coming from the intended sender.

Source of excerpt: KII3

Box 2. 6: The Dark Side of Theft

CASE STUDY

In 2020, thieves broke into our office. One evening, after closing from work on Friday, I was there on Saturday when I received a call from my landlord that thieves had broken into the office and had taken away our laptops, a Samsung laptop, all our pen drives, the Wi-Fi modem and other valuables in the office; anything that they could sell to make money except the photocopier machine. I think it's because of its size that they couldn't take it. They left the desktop computer; they didn't touch it but they took the brand-new printers. They also took the brand-new Samsung laptop that we had bought with project funding, as well as all the other necessary items, such as a television, decoder, and everything else except the photocopier machine and desktop computer.

This case highlights the threat of physical theft of office equipment, including laptops, pen drives, a Wi-Fi modem, and other valuables. Some unknown persons broke into the office of the organisation, a CBO based in Ghana and promoting community livelihood development and empowerment in partnership with some international NGOs. The CBO lost valuable equipment, including a new laptop that was purchased with project funding, and their ability to access and store important information stored on the stolen devices. This shows the need for CSOs to secure their physical office space, such as installing security cameras, alarms, or hiring security guards to protect against theft. It also highlights the need for implementing data backup measures to ensure that important information is not lost in the event of theft. Another key informant (KII5) from an NGO in Nigeria shares how traumatic it can be to lose a device containing back up data, highlighting the need to complement backup on physical devices with online storage or vice versa.

My hard drive was also stolen. It was one floppy drive I had that contained some backup information. One that served us a backup drive for the external hard drive, because in a previous training we were told to always have a backup drive. As NGOs, definitely our work revolves around software or the use of laptops. So, if your information is lost, it can be very traumatic and if there is a report that you need to send, and the deadline and then you lose your information, how will you explain to your donors? It can weigh down the trust and those two are working on a timeline. It's not a good experience.

Source of excerpt: KII18 and KII5

Box 2. 7: Malware Attack

CASE STUDY

In the excerpt below, we learn about a malware attack on a CSO's computer system. The CSO is based in Ghana. It is engaged in livelihood development. The malware was introduced to the system via a USB drive provided by someone who wanted to print a document. The malware corrupted the hard drive, causing the organisation to lose all the documents that had been saved on the system since 2016.

Somebody brought a pen drive and inserted it into our device to print out a document, and then everything just vanished from our system. We called a technician and he said that the hard disc was corrupted, and we couldn't retrieve all our documents from 2016 to date. We lost everything, so we had to buy a new hard drive to start again. It was a big blow to the organisation because there were donor files, documents, and reports that we were working on. It happened during the Christmas break, so as soon as we returned, we were hit by the crisis. We were able to recover some of our information from our emails, such as the communications we had with our donors before, and other documents and reports that we had sent through emails. We had to go to an internet café to download them and bring them back to the office to recover some of the documents on our computer. It was a big shock to us.

The organisation lost important donor files and documents, as well as reports that were in progress. The attack occurred right after a Christmas break, making it difficult for the organisation quickly and effectively. They were able to recover some information from emails, but overall, the attack had a major impact on the organisation's operation organisations in West Africa can learn from this experience by being vigilant about the potential threat of malware and taking steps to protect their computer systems. This includes being cautious when inserting USB drives into devices, especially if they have not been scanned for malware, and regularly backing up important data to ensure that it can be recovered in case of an attack. Also, it is important to have a response plan in place in case of a cyber-attack, including who to contact and what steps to take to mitigate the damage.
Source of excerpt: KII18

Box 2. 8: The Conference that Never Was

CASE STUDY

A few months ago, I received an email in my inbox requesting that my organisation attend a conference outside the country. I made preparations to attend and was asked to pay a certain amount of money. I told them I was unable to pay that amount and they said everything about the flight and everything I needed had already been paid, and that I only needed to pay for my *hotel booking, which would cost about $240. They gave me a link to communicate with the hotel management to pay that money. I contacted the hotel management and they gave me the bill and it looked very real. Later, I looked at my purse and realised I didn't have enough money, so I told them I was unable to pay the bill and asked if they could slash it down or waive it. They told me they had actually slashed it down $240 and that it was previously $480. I waited for a week and realised that I was still unable to pay the $240 they asked for. My intention was to ask them to totally waive the fee if they wanted my organisation to attend the conference. However, I discovered that the website they gave me was no longer in existence after visiting it again during my passport processing, which takes a while in Nigeria. I checked the website on Google, and it was classified as a scam. If I had paid the $240, it would have been lost.*

The experience described in the excerpt above highlights the risk of scams in Nigeria. The CSO received an email inviting their organisation to attend a conference outside the country, with the promise that the flight had already been paid for and that only the hotel booking needed to be paid. The CSO was asked to pay an amount of 240 US dollars, and provided with a link to communicate with the hotel management to pay the bill. However, the CSO later discovered that the site was a scam and that the information provided was not genuine. This experience has implications for CSOs in West Africa as it highlights the importance of being cautious and vigilant when receiving unsolicited emails and requests for payment. It is recommended that CSOs in West Africa should thoroughly verify the authenticity of any such requests, and should not make payments without verifying the authenticity of the source. This can be done by checking the reputation of the source online, checking the details of the email, and confirming the authenticity of the site through multiple sources.

Source of excerpt: KII17

Box 2. 9: Extortion and Harassment through Social Media Platforms

CASE STUDY

The following demonstrates a typical case of "social engineering". It involves the use of deception and manipulation tactics to trick an employee of a CSO into revealing sensitive information or performing actions that put their digital security at risk. In this case, the attacker posed as a community member through social media, gained the informant's trust, and then used that trust to extort money and threatened to reveal the informant's identity and the organisation's activities.

I experienced harassment on Facebook where somebody was harassing me because of my sexuality. I was chatting with somebody who posed as a community member, and who later sent my details to another guy. This person then reached out to me saying he would publish my name and pictures on all social media platforms, to expose me for being gay. He claimed to know where I worked and what my organisation did, and threatened to report us to the authorities. He demanded that I pay him 100,000 Naira or he would ruin the reputation of my organisation. After I paid the money, he continued to make more demands, so I had to delete the account and open a new one, losing all my contacts. The money I paid was for my house rent, and I am currently staying with someone else because this person threatened to come to my former residence and harass me. I am currently hiding to avoid further threats.

The excerpt describes a situation in which the informant, a member of a community-based organisation working to protect the rights of LGBT+ people in Nigeria, where being LGBT+ is illegal, experiences harassment on Facebook. The informant was chatting with someone who sent their details to another person, who then threatened to publish their name and pictures on social media and report their organisation to the security forces, unless they paid a bribe of 100,000 Naira. Despite paying the bribe, the harasser continued to threaten and extort the informant, leading the informant to lose all their contacts and even have to move out of their home to avoid the harasser. The experience perhaps highlights the vulnerability of LGBT+ people and organisations in Nigeria organisation are importantly, the potential dangers of online harassment and extortion. Other CSOs can learn from this experience to take necessary precautions to protect themselves from similar situations, including creating a clear social media policy, training staff on digital security, and having a strategy for dealing with harassment and extortion. In this specific case, the organisation had no such arrangements in place as the informant confirmed,

They [the CBO] have no idea how to go about it, … the only solution is that they just told me to deactivate the account and open a new one.

Source of excerpt: KII21

Box 2. 10: A Sister's Scandalous Scam

CASE STUDY

The incident described in the key informant interview is a case of identity theft facilitated through the use of social media. The informant's sister, who is also working in the organisation, became a victim of this scam. The scammers obtained information from the sister after she filled out a form that required personal details such as passport information and account details. The scammer then created a fake loan company and sent messages to people in the sister's contacts, claiming that she owed a certain amount of money and that she would be arrested if she did not pay it back within 15 days. People who knew the sister started paying money into the account before even sending the information to the informant.

This one was like an identity theft version of scam. This one actually happened to my own sister. You know, my sister is also working with me in the organisation. In this one here, they obtain information through a form where you have to fill in your details, put your passport and everything about you. If you have your ID card, they ask you to scan it and put it there, your account details, everything is there. The focus of this fund is to give grants. Grants have become popular in Nigeria, and if you're an NGO, they tell you that you can come up as an NGO and apply for this grant. They get your information from there, and who knows what they will use the information for. I've been a victim of that. My sister became a victim of that after sending that information to them. These fraudsters went and used that information to get in contact with my sister on Facebook and WhatsApp and also get a contact from the phone number, from that phone number. I don't know how they got the contact details of people on that sim card. With this one now, they opened a WhatsApp and then sent information to these people that my sister collected a loan from them. They pretended to be a loan company and told the people that my sister got a loan from them and refused to pay back, and they need their money. Within 15 days, they are going to arrest her if they *don't see the money. People around that know my sister said, "How can it be?" and before you know it, they started asking and interacting with the guys. They asked, "Okay, how much is she owing?" They said, "Okay, it's so-so and so amount of money." Before you know it, people that know my sister started paying money into that account. My sister was not even aware, and the funny thing is that these people did not call my sister to say, "Are you owing so-so and so amount of money with this company?" They didn't ask, they kept on paying. About 3, 4, 5 persons paid money into the account before they even sent the information to me too. When I saw it, I called my sister and said, "Ah, what happened, this one that you are... in fact, the picture of my sister's card is there. Every identity card of my sister was there." I said, "Ah, how can this happen?" I also don't know where they got another picture of my sister and they put it there too. They wrote it there neatly, and before you know it, people paid money in. When I told my sister what was happening because she was not aware, my sister decided to call them, and they blocked her. They blocked it, so any other person who called that line, it didn't go through again. That was how they duped her, and the people who paid money too later discovered that my sister didn't owe anybody. She has never for once collected a loan, and she is not owing anybody. So, my sister became a victim of that, and they went away with close to 100,000 Naira.*

The impact of this incident is significant, as multiple people ended up paying money into the fake account. The scammers used the informant's sister's picture and identity information to make it seem legitimate, which led to several people falling for the scam. The incident also highlights the importance of being cautious and verifying the authenticity of requests for personal information, as well as the potential consequences of identity theft. CSOs in West Africa must be vigilant and educate their staff on the importance of protecting personal information and the potential risks associated with sharing information online.

Source of excerpt: KII17

Appendix 3

Existing national laws and policies about digital security in West Africa (by country)

Benin

Law n° 2017-20 of April on the digital code in Benin is since 2018 recognised as the only legal framework of the digital sector in Benin. Part VI of the Act addresses Arrest, Search, Seizure, and Prosecution. For example, Section 45(1) states that a law enforcement officer may apply to a judge in chambers for a warrant to obtain electronic evidence in relation to a crime investigation. The judge may issue a warrant that authorises a law enforcement officer to take certain actions in seven different situations to prosecute digital offenses. Additionally, the Constitution of the Federal Republic of Nigeria stipulates that those who do not comply with lawful inquiries or requests made by law enforcement agencies in accordance with the Act will be considered to have committed an offense, and may face imprisonment for a term of 2 years or a fine of N500,000.00 or both such fine and imprisonment.

The Beninese legislator places great emphasis on protecting privacy. The Personal Data Protection Authority (APDP) was established to ensure compliance with legal provisions regarding the protection of personal data. Since its creation in 2009, it has only approved 300 requests for the collection or deletion of personal data and received around ten complaints UNCTAD (2015).

Burkina Faso

In Burkina Faso, the first law on data protection was passed in 2004, through the Act No. 010-2004/AN of April 20. The Commission de l'informatique et des libertés (CIL) was established as a regulatory body under this act and began operations in 2007. However, as the use of social media and cloud services became more widespread, it became clear that the 2004 law needed to be updated to reflect the current circumstances and global norms. In order to ensure that data flows were unhindered and personal safety was guaranteed, the 2004 act was repealed and replaced by a new Act No. 001-2021/AN of March 30, 2021, which was enacted on April 21, 2021. This new law makes fundamental modifications to better protect people's privacy and aligns with the ECOWAS Supplementary Act No. A/SA.1/01/10 of February 162010.

The new Act No. 001-2021/AN of March 30, 2021, which was enacted on April 21, 2021, in Burkina Faso, still requires permission for data processing, and the exception of legitimate interest of the controller or a third-party recipient is not recognised. This is because the legal justifications for data processing have not significantly changed. Additionally, the majority of ECOWAS member nations do not include this provision as it is not mentioned in the ECOWAS Supplementary Act. To align with international standards, the rights of the data subject have been enhanced, but the right to portability is not included. These rights include the right to information, which carries extensive transparency requirements, as well as the right to object, access information, make corrections, have information erased from memory, and be forgotten. If there are any legal violations involving data protection, the company will be held accountable and the penalties for such violations have been increased to be more deterrent. They can amount to 1% of a company's revenue for the first offense and 5% in the event of repeat offense.

Cameroon

In the past 20 years, Cameroon has implemented various laws and actions in the field of Information and Communication Technology (ICT). In 2016, the government created the Cameroon Digital Strategic Plan 2020, which outlined 8 strategic objectives for improving internet coverage in the country, including expanding broadband infrastructure, increasing digital content production and supply, facilitating digital transformation in government and businesses, promoting digital culture, enhancing digital trust, fostering a local digital industry and research and innovation, developing human capital and digital leadership, and improving governance and institutional support.

Over the past 20 years, Cameroon has taken steps to advance its information and communication technology (ICT) sector through laws and actions. In 2016, the government introduced the Cameroon Digital Strategic Plan 2020, which set out eight goals to improve internet coverage in the country. These include developing broadband infrastructure, boosting digital content production and distribution, promoting digital transformation in government and businesses, fostering digital culture, increasing digital trust, encouraging a local digital industry and research and innovation, developing human capital and digital leadership, and enhancing governance and institutional support.

The law also includes penalties for those who violate data privacy. As per Section 61, employees and security audit experts of corporate bodies who disclose confidential information without permission during a security audit will face imprisonment of 3 months to 3 years and a fine of 20,000 to 100,000 CFA francs. Refusing to comply with summons from authorised officials will result in imprisonment of 3 months to 4 years. Anyone who hinders, incites resistance, or prevents investigations related to this section, or refuses to provide information or documents, will face imprisonment of 1 to 5 years or a fine of 100,000 to 1,000,000 CFA francs, or both.

On the other hand, Section 62 states that anyone who falsely presents content or activity as illegal with the intention of causing its removal or stopping its publication will face imprisonment of 1 to 5 years and a fine of 200,000 to 2,000,000 CFA francs. Additionally, the publisher is required to insert a response from the person designated in the electronic communication service within 48 hours of receipt, or face a fine of 100,000 to 2,000,000 CFA francs.

Cape Verde

Law 133/V/2001, established on January 22nd, serves as the foundation for cybersecurity in the country. This law sets the legal guidelines for the protection of individuals in regard to the handling of personal data. Specifically, Article 1 of this law establishes the general legal framework for the protection of individuals in regards to the handling of personal data.

Section 9 covers topics like suspicion of illegal activities, penalties, security measures, and violations. For instance, it permits the CNPD to handle data regarding individuals suspected of illegal activities, and to authorise decisions regarding penalties, security measures, fines, and additional penalties, as long as data protection rules and information security are adhered to and the processing serves the legitimate interests of the controller and does not infringe on the fundamental rights and freedoms of the data subject.

Additionally, the handling of personal data for police investigations will be limited to what is necessary to prevent a specific threat or prosecute a specific violation and to fulfil the responsibilities outlined in relevant laws or international agreements to which Cape Verde is a party.

Chad

According to Piper (2023), in Chad, the regulations concerning the protection of personal data are mainly governed by several laws and protocols. These include Act No. 007/PR/2015 of February 10, 2015, which pertains to Personal Data Protection, as well as Decree No. 075/PR/2019 of January 21, 2019, which implements the provisions of the aforementioned act. Additionally, Act No. 006/PR/2015 establishes the National Agency for Computer Security and Electronic Certification, and Ordinance No. 002/PR/2019 amends this act. Furthermore, Ordinance No. 009/PCMT/2022 also amends Act No. 006/PR/2015. Other relevant legislations include Act No. 009/PR/2015 on cybersecurity and the fight against cybercrime, Ordinance No. 008/PCMT/20022 on cybersecurity in the Republic of Chad, and Act No. 008/PR/2015 on electronic transactions.

In Chad, the Agence Nationale de Sécurité Informatique et de Certification Électronique (ANSICE) serves as the National Data Protection Authority. ANSICE is responsible for ensuring compliance with the provisions of the Act on a national level and has the authority to sanction any violations of the Act. Its key responsibilities include informing data holders and controllers of their rights and obligations, receiving formalities prior to the creation of personal data processing, and other related duties. While there is no nationwide registration system in Chad, the processing of personal data may require prior notification or authorisation/approval from the CDP. The Act does not have any specific provisions pertaining to the appointment of Data Protection Officers (DPOs), and this issue is solely at the discretion of the data controllers.

In Chad, data collection and processing are required to adhere to a set of principles and requirements. Personal data must be lawfully, fairly, and transparently collected, recorded, processed, stored, and transmitted. Additionally, data must only be collected for explicit and legitimate purposes, and must be relevant and not excessive for the intended use. Personal data should not be kept for longer than necessary. Data Controllers are responsible for ensuring the security of personal data and must take measures to prevent unauthorised access, alteration, and damage to the data. Access to the data system should only be granted to authorised personnel, and third-party recipients must be verified. Breaches of data privacy may lead to judicial penalties such as imprisonment for one to five years, as well as fines ranging from XAF 1 million to XAF 10 million, as per Article 438 of the Criminal code.

Kalemera et al. (2020) indicated that although freedom of expression is constitutionally protected in Chad, laws and regulations on contempt and defamation have been used to silence critics of the government both online and offline over the past two decades. The press regime law of 2010 introduced criminal penalties for defamation, with fines ranging from 10,000 CFA francs (16.8 USD) to 500,000 CFA francs (840.6 USD) and the possibility of suspension for up to three months upon conviction. Defamation is defined as any statement or accusation likely to harm the reputation or dignity of an individual or organisation. Despite the removal of prison terms for defamation, this provision has been used to restrict criticism of government officials and limit freedom of expression.

Côte d'Ivoire

The Ivorian government has taken action to combat the increasing number of cybercrimes committed by its citizens against victims in French-speaking countries such as Côte d'Ivoire, Switzerland, France, Belgium, and Canada by adopting several cyber laws. The Fight Against Cybercriminality Act (No 451) was passed in conjunction with The Law No. 2013-450 on The Protection of Personal Data. The first article of the Fight Against Cybercriminality Act states that definitions of legal instruments from ECOWAS, the African Union, or the International Telecommunication Union will apply to terms not defined in the act. This provision is significant as it enables the implementation of the African Union Convention on Cybersecurity and Personal Data Protection, which was adopted by the African Union in 2014 in Malabo, Equatorial Guinea.

The second article of the Law lays out the purpose of the Law, which is to combat cybercrime and criminal offenses that require the collection of electronic evidence. The Act is divided into 8 chapters, covering topics such as crimes specific to Information and Communications Technologies (Chapter 3), penal procedure in cybercrime (Chapter 8), offenses to intellectual property (Chapter 4), illegal acts on electronic communication networks (Chapter 5), obligations of Internet Service Providers (Chapter 6), and the application of traditional offenses to Information and Communication Technologies (Chapter 7). Chapter 3 of the Act establishes the penalties for committing crimes related to information systems and the internet in general.

The act of fraudulently accessing or attempting to access an information system (Art. 4) is punishable by imprisonment of up to 2 years and a fine of $10,000 to $20,000. Fraudulent interception of computer data or an attempt to do so (Art. 8) is met with severe penalties, including a prison sentence of up to 10 years and a fine of between $80,000 and $120,000. These penalties are significant deterrents for the average cybercriminal operating in Côte d'Ivoire.

The alteration, modification, or suppression of computer data (Art.9) is heavily punished by imprisonment of 10 years and a fine of $120,000. It's worth mentioning that Chapter 3 of the Fight Against Cybercriminality Act is the core of the law and comprises of 30 articles. Additionally, Article 13 of the Act prohibits the production, sale, or distribution of computer programs, passwords, access codes, or similar computer data. This is punishable by up to 2 years in jail and a fine of $100,000. For comparison, Art. 23 of the Cybercrime prevention and prohibition Act of 2015 in Nigeria punishes those who engage in the production and distribution of child pornography with a jail term of no more than 15 years, which is 3 times greater than the jail term in the Ivorian legislation, although the fine in the Nigerian legislation is $49,000.

Gambia

The National Cybersecurity Strategy and Action Plans 2016 emphasised the need for swift development of cybercrime legislation. The strategy includes some general requirements that need to be evaluated, and some legislative improvements are currently being implemented. This includes a review of the Information and Communications Act of 2009.

Additionally, the Information and Communication (IC) Act 2009 has provisions for significant offenses. Part III of Chapter III of the existing IC Act 2009 deals specifically with Computer Misuse and Cybercrime, while Part IV of the same chapter focuses on the protection of children. Furthermore, Part V of Chapter III of the existing IC Act 2009 includes provisions on procedural elements, mainly pertaining to the retention of information (Art. 181Art.182). The legislative text does not suggest provisions for electronic evidence. However, Part V of Chapter III does introduce the concept of electronic records and their use in legal proceedings.

In July 2013, the legislation governing Information and Communication Technology

(ICT) was amended, specifically the 2009 Information and Communication Act (ICA). The amendments to the ICA criminalise online dissent, where individuals convicted of "criticising, impersonating, or spreading false news about public officials" online can face penalties of up to 15 years in prison and/or fines of up to Gambian Dalasi (GMD) 3 million (USD 100,000) under these provisions. These amendments were introduced as a measure to intimidate citizens, journalists, and potential whistle-blowers from seeking legal recourse for human rights violations by the then government. According to Freedom Houses' 2014 Freedom on the Net report, the government introduced the ICA amendments in response to online activism and the growing influence of online media, particularly from the diaspora.

In December 2015, the previous government announced plans to establish a new National Cyber Security Strategy, which would include monitoring cyber threats among other things. Initial documents revealed that the strategy would address personal data protection, electronic transactions, electronic records and signatures, and computer misuse and cybercrime, which are all currently regulated by the ICA 2013 (CIPESA, 020).

Ghana

As cyber-attacks on critical information infrastructures (CIIs) continue to rise, Act 1038 provides the legal foundation (specifically Sections 35 to 40) for implementing measures to protect Ghana's CIIs. In line with Section 35 of the Act, 13 sectors have been identified as Ghana's CII sectors, including National Security and Intelligence, Information and Communications Technology (ICT), Banking and Finance, Energy, Water, Transportation, Health, Emergency Services, Government, Food and Agriculture, Manufacturing, Mining, and Education. Several institutions in both the public and private sectors have been notified of their designation as Critical Information Infrastructure Owners across these 13 sectors.

In 2008, Ghana signed the Electronic Transactions Act (ETA) to provide laws against cybercrime and enacted the Mutual Legal Assistance Act (MLAA) in 2010 to support international cooperation in cybercrime and electronic evidence. Currently, Ghana is in the process of joining the Budapest Convention. The government of Ghana passed its Data Protection Act in 2012 which offers a flexible approach in defining personal data and the legal handling of data compared to the stricter standards adopted by many African countries after the implementation of GDPR.

Ghana's new Cybersecurity legislation is seen as a significant step towards advancing the country's cybersecurity development. The Cybersecurity Act of 2020 (Act 1038) was legally enacted on December 29, 2020, after it was passed by Parliament on November 06, 2020. The Act establishes the Cyber Security Authority (CSA), creates a comprehensive legal framework for the protection of the country's critical information infrastructures, regulates cybersecurity activities such as licensing cybersecurity services, ensures the protection of children on the internet and develops Ghana's cybersecurity ecosystem. It is also aimed at enabling Ghana to prevent, manage, and respond to cybersecurity incidents as the country undergoes digital transformation (GoG, 2021).

Although classified as a misdemeanor, the punishment for misdemeanor under section 296 of the Criminal Procedure Act states that the penalty for misdemeanor can be a punishment of up to three years' imprisonment, which would be excessive if the maximum sentence were to be imposed. Similarly, section 76 of the Electronic Communications Act prohibits the act of knowingly sending false or misleading communication that could potentially harm the efficiency of life-saving services or endanger the safety of individuals, ships, aircrafts, vessels, or vehicles, by means of electronic communication. The penalty for violating this section is a fine, imprisonment up to a maximum of five years, or both UNCTAD (2015).

Guinea

The Guinean government recognises the benefits of Information and Communication Technologies in reducing time constraints, physical borders, developing and maintaining business relationships, and increasing the productivity and performance of industries and services. However, it also acknowledges that cyber development poses many complex challenges for states, and that cyberspace can be used to commit serious reprehensible acts without borders.

For Internet Without Borders, the fight against cybercrime is necessary to create a secure cyberspace for citizens, but it must be done in strict compliance with the principles of proportionality, necessity, and legality. Additionally, with the increasing presence of digital companies in Africa, *Internet Without Borders* is in favour of African states legislating on the protection of personal data and the privacy of their citizens. The Law L2010/003/CNT of June 23, 2010, creates a Guinean "High Authority for Communication" whose mission is to ensure "compliance with the principle of equality of communication users; respect for plurality, the expression of currents of thought and opinion in public communication services." The HAC states on its website that it is "an organisation that defends citizens' right to information" and has a role of supporting and mediating to avoid any abusive control of the media by the government or manipulation of public opinion through the media.

The first law on the general regulation of telecommunications in Guinea was established on June 2, 1992, and was later amended by Law L/2005/018/AN on September 8, 2005. On August 13, 2015, Law No. L/2015/018/AN on telecommunications and information technology, also known as the new telecommunications law, was enacted. Both laws include provisions for respect for personal data and privacy. The 2005 law includes penalties for "any agent of a telecommunications network operator or telecommunications service provider who refuses to provide information or documents or obstructs investigations" (Article 48).

The association states that "Articles 70 and 71 require telecommunications operators, and digital companies, to act as censors, forcing them to provide devices to filter content accessible to Internet users, under penalty of fine or even imprisonment". In 2019, the private press union opposed the use of Article 31 of the cybercrime law to repeatedly summon journalists. After four days of intense work, the Republic of Guinea validated a national policy and strategy document on Cybersecurity on April 7, 2019. This document serves as a reference for cybersecurity policy and strategy and outlines the main legal and regulatory guidelines for the next five years (2022 to 2027).

Guinea-Bissau

Guinea-Bissau's Law No. 5/2010, known as the Basic Law on Information and Communication Technologies, provides legal guidelines for the development and regulation of the ICT sector, but does not address cybersecurity in the country. According to the African Union Commission and Symantec (2016), Guinea-Bissau has no specific legislation concerning cybercrime, and there is no official national or sector-specific cybersecurity framework to implement internationally recognised standards. While there are legislative initiatives in progress, there are currently no laws in place relating to electronic commerce or activities in cyberspace.

Liberia

According to Badio and Dillon (2017), there is currently no law in Liberia specifically addressing cybercrime issues. However, provisions in the existing Electronic Transactions Law (ETL) address cybersecurity issues related to authentication and integrity through certification authorities. In 2019, the Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA) was established as a non-governmental agency to provide cyber security and digital forensics education to the government and people of Liberia. The agency was officially recognised by the Ministry of Justice to implement its mandate in the areas of supporting government and private entities initiatives in the fields of cyber security and digital forensics.

The mission of the Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA) is to strengthen the ability of public and private institutions in Liberia to prevent and address cybercrime through policy development, training, and awareness raising. The agency uses a proactive approach to provide cyber and digital forensics training, promote cyber security education, and create a safer online environment for citizens. They also provide technical assistance to judicial and law enforcement agencies, develop standards and strategies to combat cyber risks, conduct cybercrime assessments, and offer cyber defensive capabilities to the business community. The agency's efforts are particularly important given Liberia's vulnerability to cybercrime, which is exacerbated by factors such as lack of awareness and a lack of national legal and regulatory framework for cybercrime.

As of now, Liberia has no specific legislation in place to address cybercrime issues. The Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA) is a non-governmental organisation established in 2019 to provide cybersecurity and digital forensics education to the government and citizens of Liberia. The forum focuses on raising awareness for cybersecurity and its implications for government, businesses, and society. However, institutions such as the Central Bank of Liberia and the Ministry of Post and Telecommunications have developed policies aimed at preventing or mitigating the effects of cybercrime. Despite the recognition of the threat posed by cybercrime on the global community, Liberia has no national legislation on cybercrime. The National Telecommunications and ICT Policy 2010-2015, developed by the Ministry of Post and Telecommunication, does not discuss elements related to cyber offenses and cybercrime.

To address the lack of specific legislation on cybercrime in Liberia, the Liberia Telecommunications Sector has drafted a law that incorporates provisions from the Ecowas Supplementary Act on Cyber Security. This law includes legal grounds to prosecute individuals who commit cybercrimes in Liberia. The draft law is currently undergoing final review and once completed, it will be presented to the National Legislature for approval and passage into law.

Mali

According to Toussi (2020), on December 5, 2019, the President of Mali passed Law n° 2019-056 on the Suppression of Cybercrime. While it is a timely and relevant legislation, several provisions pose potential risks to privacy and freedom of expression online, particularly given Mali's shortcomings in democracy and low press freedom ranking. The law applies to "any offense committed by means of Information and Communication Technologies (ICT) in whole or in part on the territory of Mali, or any offense committed in cyberspace and whose effects occur on the national territory." It is part of a legislative framework aimed at supporting reforms in the technology sector, as outlined in the 2000 Mali Telecommunications Sector Policy Declaration.The Telecommunications Act of 1999, in Article 1, supports the constitutional provision of privacy. However, the Cybercrime Law, in Articles 74 to 78, allows for searches of computers and seizure of data as part of criminal investigations, which conflicts with this established right to privacy. Additionally, Article 75 allows for copying and storing data if "seizure of the medium seems inappropriate." The law does not provide guidance on how the copied data should be stored, processed, or disposed of once investigations have concluded. This undermines the principle of data protection outlined in Article 7 of the Personal Data Protection Act, which stipulates that personal data should only be kept for a specified period and purpose.

Additionally, articles 83 to 86 provide for real-time surveillance through the interception of communications. Service providers are required to cooperate with authorities by ensuring they have the necessary technical means in place to facilitate the interception of communications. These broad powers are in addition to those given to authorities under Article 4 of the Telecommunications Act, which allows the government to requisition all telecommunications networks and equipment in the territory of Mali, and/or prohibit the provision of telecommunications services for a limited period when it is deemed necessary for public security or defence. This article has been invoked in the past, such as when the government ordered social media disruptions in 2016 during public protests and internet shutdown during the 2018 elections.

Furthermore, communications service providers are required to put in place mechanisms to monitor systems for potential illegal activity, with failure to inform authorities of illegal activities being punishable by a prison sentence of between six months and two years, a fine of Central African Francs (CFA) 500,000 to 2,000,000 (USD 830 to 3,318) or both (article 25). The law aims to ensure safe and secure use of ICT in Mali, but it is implemented in a fragile context. Provisions related to data processing as part of criminal investigations pose significant risks to personal data integrity, security, and privacy. Also, the law places a heavy burden on telecommunications intermediaries to track and monitor network activity and holds these intermediaries liable for the actions of their clients. Provisions related to online press offenses are inconsistent with the legislation of media in the age of digitalisation. The new law and existing related laws therefore require revisions to safeguard and uphold constitutional guarantees of freedom of expression and privacy, online and offline.

Mauritania

Prior to 2016, Mauritania did not have a specific law dedicated to cybersecurity, which created a significant gap in legal provisions for combating cybercrime. The absence of such provisions posed a potential threat to the implementation of any ICT-related strategy (United Nations Institute for Disarmament Research (UNIDIR), (2019)).

Despite this, Mauritania's personal data protection is governed by Law No. 2017-020 of 22 July 2017, which is not yet in effect. To come into force, a new law must be accompanied by an implementation decree under Mauritanian law. Until this happens, the law aims to regulate the processing of personal data on Mauritanian soil or in any area where Mauritanian law applies, but excludes personal data processing carried out for non-dissemination purposes and data in transit.

The creation of the Autorité de Protection des Données à caractère personnel (APD) in Mauritania is provided for by the Data Protection Authority Law No. 2017-020, but the APD is currently not functional. Its primary responsibility will be to guarantee that the processing of personal data does not compromise the public freedoms and privacy of individuals in the Republic of Mauritania.

The protection of personal data in Mauritania is addressed in Draft Law No. 2017-020, which outlines requirements for data processing and data subject rights. The law also lays the foundation for the establishment of a Personal Data Protection Authority, but as of now, such an authority has not been established. Although the Draft Law was approved by the National Assembly on 22 June 2017, progress towards its implementation has been limited.

In his review of 2015-2017 and plan for 2018, the Prime Minister indicated that the legal basis for Mauritania's information society had been established, including the formation of a data protection authority and an electronic certification authority. However, concrete developments in this regard have been few and far between. Recent discussions have centered around improving the use of FinTech and personal data protection in the financial sector (Dataguidance, 2017).

It remains to be seen if and when the Draft Law will come into effect, how it will be implemented, and whether the Prime Minister's proposed foundations will be built upon. It is worth noting that Mauritania is one of several jurisdictions that have signed but not yet ratified the African Union Convention on Cyber Security and Personal Data Protection.

However, presently, cybercrime in the country is governed by Law 2016-007. For instance, Article 5 of the law outlines penalties for individuals who intentionally and without authorisation damage, erase, deteriorate, alter, or delete computer data. Offenders may face imprisonment for up to three years and a fine ranging from 100,000 to 2,000,000 ouguiyas, or one of these two penalties (United Nations Institute for Disarmament Research (UNIDIR), (2019)).

Nigeria

Nigeria introduced its National Security & Cybersecurity policy in 2014. The goals of this policy include creating a security strategy that adapts to the changing national security threat landscape, and reducing national risk exposure and uncoordinated presence in cyberspace.

One of the key areas of focus of the policy is to establish a legal framework that defines the government's responsibilities in ensuring cybersecurity. The policy outlines eleven points that explain the Nigerian Government's role in combating cybersecurity while protecting Nigerians who operate online. For instance, it states that the government has the responsibility of taking legal and regulatory actions to improve and update federal and state laws to combat cybercrime.

To provide a more specific legal framework, Nigeria passed the Cybercrimes (Prohibition, Prevention, etc.) ACT, 2015. This act provides a unified, comprehensive legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes in Nigeria. It also aims to protect critical national information infrastructure, promote cybersecurity, and protect computer systems and networks, electronic communications, data, computer programs, intellectual property, and privacy rights. The objectives of the Act, outlined in Part I, are that the provisions of this Act should apply throughout Nigeria.

Similarly, Part VI of the Act deals with Arrest, Search, Seizure, and Prosecution. For instance, Section 45(1) states that a law enforcement officer may request a judge in chambers to issue a warrant for the purpose of obtaining electronic evidence in related crime investigations. A judge may issue a warrant authorising a law enforcement officer to take certain actions in seven different situations to prosecute digital offenses. According to the Constitution of the Federal Republic of Nigeria, failure to comply with lawful inquiries or requests made by law enforcement agencies in accordance with the provisions of this Act is considered an offense and may result in imprisonment for a term of 2 years or a fine of up to N500,000.00 or both such fine and imprisonment.

Niger

Niger has taken significant steps towards creating a legal framework for digital security in recent years. The country has implemented several laws and regulations governing data protection and cybersecurity to ensure the safety and security of its citizens. According to UNCTAD's Cyberlaw Tracker[11], Niger has four main legislations governing Electronic Transactions, Consumer Protection, Privacy and Data Protection, and Cybercrime. The High Authority for the Protection of Personal Data (HAPDP) is responsible for enforcing these laws and ensuring compliance with data protection regulations. The HAPDP website[12] provides a comprehensive list of the national legislations related to digital security.

One of the primary laws governing data protection in Niger is Law No. 2019-20 of July 19, 2019, relating to the protection of personal data. This law regulates the processing of personal data and aims to protect individuals' fundamental rights and freedoms. It requires data controllers to obtain prior consent from individuals before processing their personal data and outlines the individuals' rights, including the right to access, rectify, and delete their personal data.

Another important legislation is Decree No. 2018-176 of March 5, 2018, on the organisation and operation of the National Agency for Computer Security (ANSI). This decree establishes the ANSI, which is responsible for ensuring the security of Niger's computer systems and networks. The agency is also charged with developing cybersecurity policies and strategies, coordinating and implementing cybersecurity measures, and promoting awareness of digital security among the public and private sectors.

Niger has also implemented laws related to cybercrime. For instance, Law No. 2019-21 of July 19, 2019, on cybersecurity and the fight against cybercrime criminalises various cyber activities, such as unauthorised access, hacking, and identity theft. The law imposes severe penalties, including imprisonment and fines, for those found guilty of committing cybercrime. Additionally, Law No. 2021-15 of June 8, 2021, establishes the National Authority for the Fight Against Cybercrime (ANLC), which is responsible for coordinating and implementing measures to combat cybercrime in Niger.

Niger has also taken steps to ensure that digital security is a priority in the country's public and private sectors. In 2019, the government implemented Decree No. 2019-491 of October 16, 2019, on the establishment of a national cybersecurity committee. This committee is responsible for developing and implementing a national cybersecurity strategy, promoting awareness of cybersecurity among the people, and coordinating cybersecurity measures between different government agencies.

Overall, Niger has made significant progress in creating a legal framework for digital security.

[11] See UNCTAD. (n.d.). Cyberlaw Tracker - Niger. Retrieved February 28, 2023, from https://unctad.org/page/cyberlaw-tracker-country-detail?country=ne

[12] See Haute Autorité de Protection des Données à Caractère Personnel (HAPDP). (n.d.). Législation nationale [National legislation]. Retrieved from https://www.hapdp.ne/legislation-nationale/

The country's laws and regulations regarding data protection and cybersecurity aim to ensure the protection of individuals' personal information and combat cybercrime. With the establishment of agencies such as the HAPDP, ANSI, and ANLC, Niger seems well-positioned to promote and enforce digital security across the country.

Senegal

The National Cybersecurity strategy 2022 (SNC2022) in Senegal outlines the country's vision and goals for cybersecurity, which align with the objectives and priorities of SN2025. This strategy has several main components such as: The government's vision for cybersecurity and the strategic goals to be achieved; the general principles, roles, and responsibilities that will support the implementation of this strategy; and a logical framework for putting the strategy into action, including an assessment of the current and future cybersecurity threats in Senegal. The overarching vision of SNC2022 is to create a cyberspace of confidence, security, and robustness for all in Senegal by the year 2022.

When implementing the National Cybersecurity strategy 2022 (SNC2022), the Senegalese government will adhere to the following principles. The main laws that regulate data protection in Senegal are: Law No. 2008-12, dated January 25, 2008, which pertains to the protection of personal data, also known as the "Data Protection Act" or "DPA"; Decree No. 2008-721, dated June 30, 2008, which pertains to the application of the DPA and Law No. 2016-29, dated November 8, 2016, which amends the penal code. These laws provide the legal framework for data processing, data subjects' rights and data controllers' obligations. The DPA and its application decree set forth the terms and conditions for data protection in Senegal.

When cybercrimes are committed, sanctions are enforced to hold the perpetrator accountable. The maximum criminal punishment for security breaches under the law is imprisonment for one to seven years, a fine of XOF 500,000 to XOF 10,000,000, or both. In addition, an administrative punishment of between 1 million and 100 million XOF may be imposed by the CDP (Commission de Protection des Données Personnelles) as a regulatory body.

Sierra Leone

According to the Sierra Leone National Cyber Security and Data Protection Policy 2017 – 2022, defence and protection begin with deterrence. This holds true in cyberspace as well as in other areas. To achieve the vision of a nation that is secure, resilient to cyber threats, and prosperous and confident in the digital world, the policy aims to discourage and deter those who intend to harm the country and its interests. To accomplish this, the policy aims to continue to improve cyber security levels, making it more difficult and costly for attackers to steal from or harm the country in cyberspace. The policy recognises the need to raise the cost, increase the risk, and reduce the reward for cyber-criminal activity.

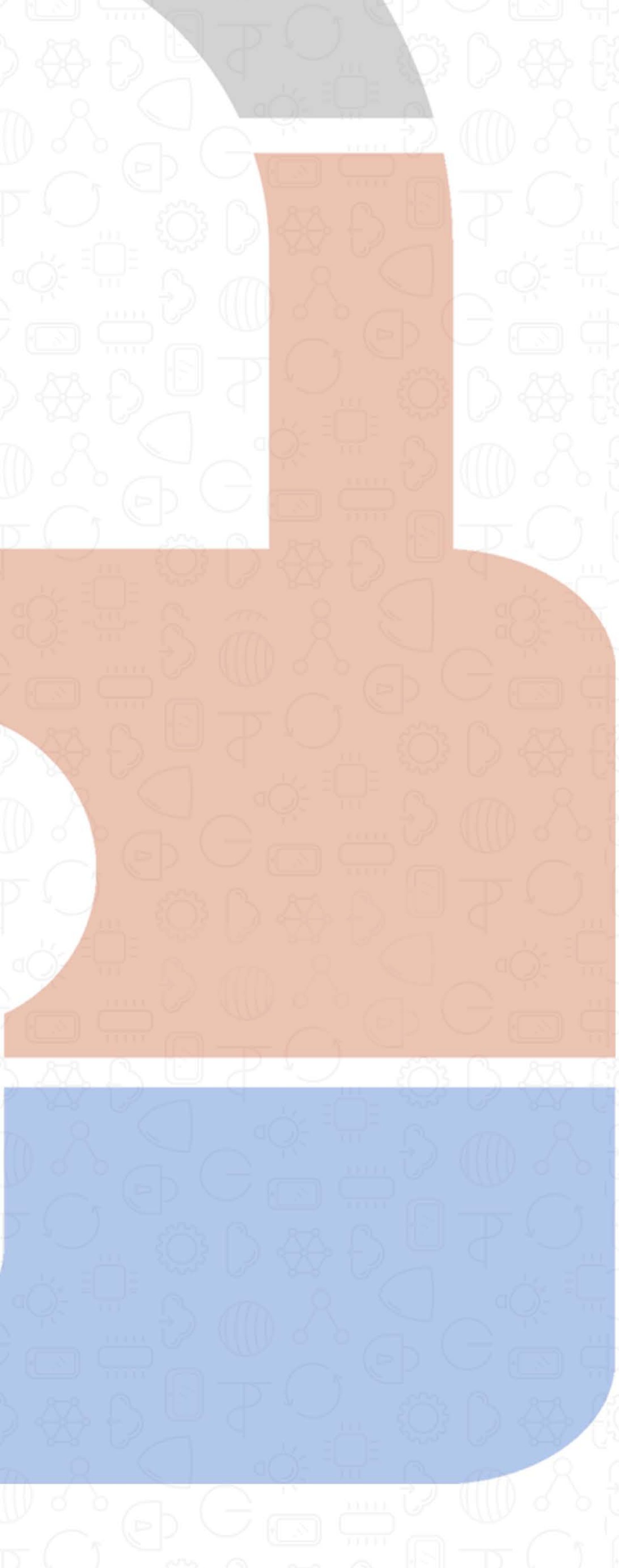
The government aims to collaborate with both domestic and international partners to target criminals and dismantle their infrastructure and facilitation networks, regardless of their location. Law enforcement agencies will continue to work towards raising awareness and standards of cyber security in partnership with the CIRT-SL (Computer Incident Response Team - Sierra Leone). The goal is to minimise the effects of cybercrime on Sierra Leone and its interests by deterring cyber criminals from targeting the country and relentlessly pursuing those who persist in attacking it. To achieve this, the government intends to take various measures, including among others that the government plans to strengthen the abilities and skills of law enforcement at the national, regional, and local levels to identify, pursue, prosecute, and deter cyber criminals both within Sierra Leone and abroad. It also aims to discourage individuals from becoming involved in cybercrime by building on early intervention measures. Additionally, the government intends to establish a 24/7 reporting and triage capability in Action Fraud, which will be linked to the CIRT-SL (Computer Incident Response Team - Sierra Leone), crime agencies, and the wider law enforcement community. This will improve support for victims of cybercrime, provide a faster response to reported crimes, and offer enhanced protective security advice. The Government will determine its success in decreasing cybercrime by evaluating progress towards specific objectives, such as increasing the disruption of cyber criminals targeting Sierra Leone, leading to more arrests and convictions, and dismantling more criminal networks as a result of law enforcement actions. Additionally, the government will aim to improve the capabilities of law enforcement, including increasing the capacity and skills of specialised officers and mainstream officers, and enhancing the capabilities of overseas partners. The Cybercrime Act of 2020 outlines specific offenses, such as unauthorised access to a computer system, which can result in fines or imprisonment as prescribed by regulation.

Togo

The legal framework for the internet is in the process of being developed in Togo. In recent years, there has been a growing focus on digital activities among legislators. In 2018, Togo's parliament passed a law on cybersecurity and cybercrime. The following year, the Personal Data Act was established on October 29, 2019, to protect personal data.

The law on the identification of natural persons in Togo (e-ID Togo), which was passed by the Togolese parliament on September 3, 2020, established the legal framework for biometric identification data. This law outlines mechanisms to regulate the management of citizens' biometric data and is the second law that governs personal data in Togo. It's worth noting that the drafting of laws and policies is not widely communicated to the public, to allow citizens provide feedback and familiarise themselves with the content of the laws. Togo signed the African Union Convention on Cybersecurity and Protection of Personal Data (Malabo Convention) on April 2, 2019, and has subsequently ratified it.

At the sub-regional level, Togo is a party to the Additional Act A/SA.1/01/10 on the protection of personal data within the ECOWAS legal system. It is worth noting that Togo's laws are in compliance with international legal commitments UNCTAD (2015).



www.wacsi.org

WACSI
WEST AFRICA CIVIL SOCIETY INSTITUTE

CHARLES STEWART
MOTT FOUNDATION®