WACSeries Op-Ed
No. 8 - October 2019

Enhancing Digital Security Awareness for CSOs in Africa

By Elongué Christian & Sule Anthony

AUTHORS

Elongué is an Afropolitan and bilingual professional who serves as Knowledge Management Programme Officer at WACSI. He has over 7 years' experience as a debate trainer, instructional designer and communications professional with leadership experience in both the public, private and civil society sectors. He is a 2013 Certified World Debate Institute' Trainer (USA), an Ashoka Changemaker Fellow and 2018 Alumni of Aileen Getty School of Citizen Journalism from the European Union Peacebuilding Initiative. He is a member of the Alliance for Nonprofit Management (USA) with research interests in cyber-security, women leadership, African philanthropy, civil society sustainability and social movement.

Sule Anthony is a digital security strategist, trainer and incident responder with a core focus in public interest. Currently, he works as the Project Manager, Digital Security at Co-Creation Hub Nigeria, where he leads the development and implementation of digital safety strategies and programs for at-risk organisations and communities, and majors in responses such as Vulnerability Assessment, Digital Forensics, Incident Response, Training and Security Consultation.

Editorial Team
Jimm Chick Fomunjong - Head, Knowledge Management Unit, WACSI
Franck Sombo – Head, Monitoring Evaluation and Learning, WACSI
Brencil Kaimba – Advisory Board Member of the International Council of E-Commerce Consultants (EC-Council) & Editor in Chief of 2019 Africa Cybersecurity Report.

About WACSI
The West Africa Civil Society Institute (WACSI) was created by the Open Society Initiative for West Africa (OSIWA) to reinforce the institutional and operational capacities of civil society in the region. WACSI also serves as a resource centre for training, research and documentation, experience sharing and political dialogue for CSOs in West Africa.

About WACSeries
WACSeries are analytical periodic write-ups on topical themes and issues relevant to West Africa. These write-ups provide experts, researchers and practitioners a space to reflect, analyse and posit views and recommendations on emerging issues and debates.
The WACSeries Op-Eds are thought provoking and intellectually engaging write-ups that provide critical reflections and analysis of issues relevant to civil society and development in West Africa.

Objectives of WACSeries
- To raise awareness on key issues in West Africa;
- To generate debates and discussions on these issues;
- To proffer recommendations on civil society involvement in advocacy;

Enhancing Digital Security Awareness for CSOs in Africa

Copyright WACSI 2019

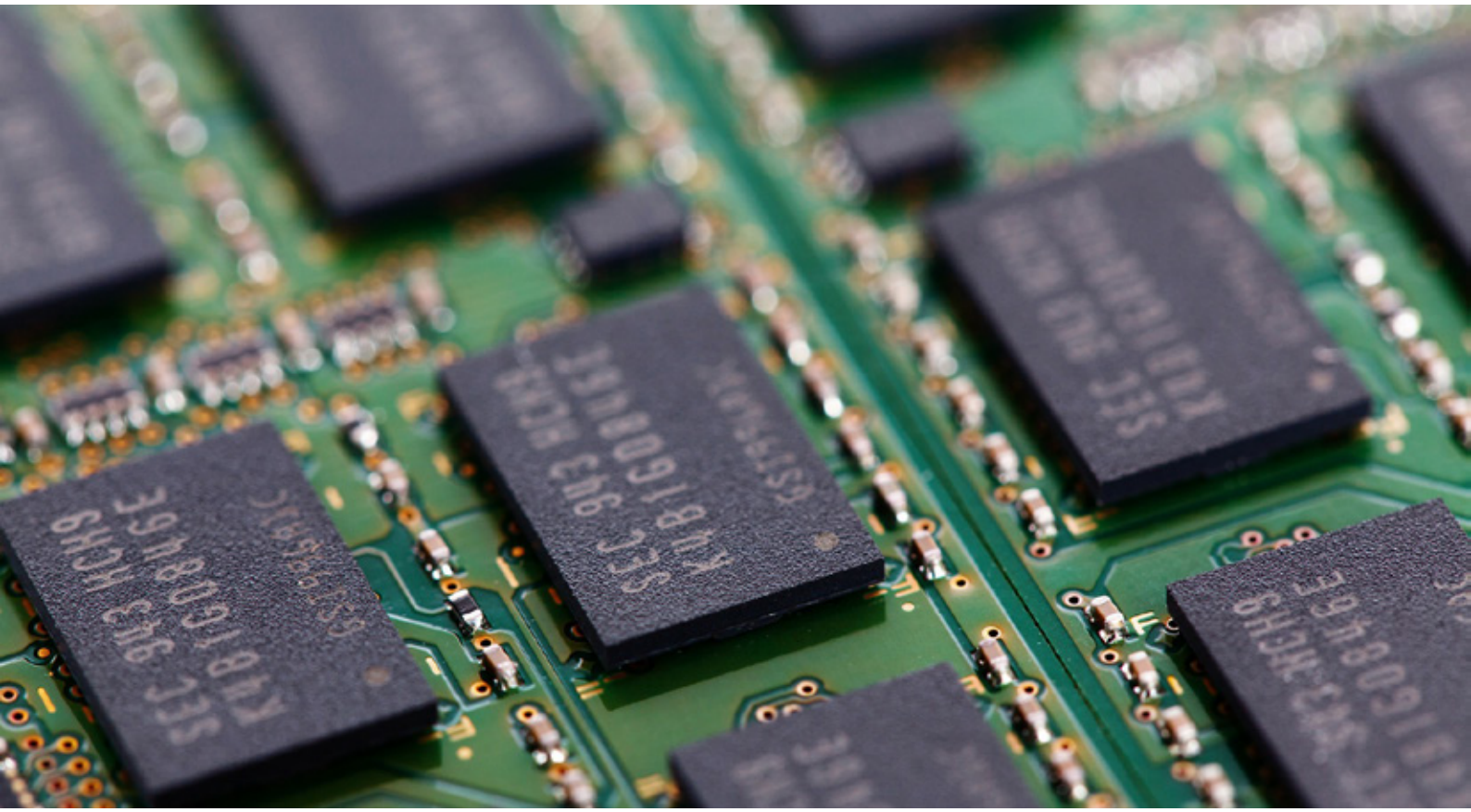
All rights reserved. No part of this report may be used or reproduced in any manner whatsoever without written permission of the Institute except in the case of brief quotations embodied in critical articles and reviews. The Institute requests the use of information in this report be registered with them for impact assessment purposes.

Disclaimer:
WACSI accepts no responsibility for suitability of any materials submitted by the contributors of this publication. WACSI assumes no responsibility or liability for errors or inaccuracies. Contributors accept all responsibility for opinions expressed. Use of this research report constitutes acceptance and understanding of these disclaimers.

For more information, write to:
West Africa Civil Society Institute (WACSI) No. 9 Bamboo Street (Formerly Bingo Street), East Legon P.O. Box AT 1956, Achimota Accra, Ghana
Email: research@wacsi.org Tel: +233 (0) 303 937 264

Cite as:
Elongué, C., Sule, A. (2019), Enhancing Digital Security Awareness for CSOs in Africa, WACSeries Op-Ed No. 8 - October 2019, West Africa Civil Society Institute, Accra, Ghana.

To contribute to this WACSERIES publication,
contact : research@wacsi.org
+233(0)501440545



Introduction

Over the last two decades, technology tools available for civil society actors in Africa have tremendously evolved. Journalists and activists relied mostly on print media to call out dictators and authoritarian regimes. To avoid being incarcerated, they hid their identities or never stayed in one location. Today, they use digital technologies to mask their identities and digital footprints, and communicate in real-time with informants and reporters using technologically advanced tools . To keep pace with the world and be effective in the work that they do, such media and civil society actors have had to embrace new and emerging technologies to facilitate their work. They make use of technological options like cloud, virtual private network (VPN), servers, WhatsApp, biometrics, co/remote working, payment gateway, among others.

The Global NGO Tech Report points out that, in 2018, 74% of civil society organisations (CSOs) including non-governmental organisations (NGOs) in Africa now operate their own websites and 55% receive donations through these websites, most of which are direct debit card payments. As many as 85% of NGOs in Africa have adopted the use of social media (mostly Facebook and Twitter) to engage and disseminate information to followers. And almost 60% regularly send email updates about their work and projects, and at least 35% adopt either WhatsApp or Facebook to communicate with supporters and donors.

This massive adoption of technology comes with gains as well as issues and challenges. Technology ultimately serves to bridge the gap between people and businesses. It connects and interfaces lives, infrastructures and processes in society. However, technology puts sensitive data and information closer to users, making the data and its users more vulnerable to cyber-attacks. Boles (2013)[1] argues that civil societies are some of the least aware of this.

1 Brianna Boles, 'Technology's Role in the Non-profit Sector: Increasing Organisational Effectiveness and Efficiency through Technology Innovations', 2013.

1. African CSOs' Awareness of Digital Attacks

Between April 2017 and April 2019, Co-Creation Hub, a social enterprise headquartered in Lagos Nigeria, conducted security vulnerability assessments for 30 CSOs across seven (7) cities in Nigeria and Ghana. The results from the assessments showed several patterns of digital security flaws in six (6) categories[2]. The most commonly identified issue across the 6 categories of CSOs assessed was: 'awareness of their own risks and vulnerabilities'.

Of the 30 CSOs, only 3 (one in Ghana, two in Nigeria) showed a level of self-consciousness in security awareness that was ranked above average. That's exactly 10% (from a collection of the strongest, most active CSOs in the two countries). Also, 24 of the assessed organisations have been victims of some form of cyber or physical attack, in the form of business email compromise, financial hack, targeted device theft and data exfiltration.

The stakes are higher now than ever. In Africa, many civil society actors, activists and journalists face targeted digital threats and cyber-attacks, threatening the security of the people working with them. In 2009, the Arab Spring illustrated the possibilities and vulnerabilities of online democracy and human rights activism. The release of the Pegasus spyware operations report in 2018 by Citizen's Lab, and the WhatsApp video call spying in May 2019, revealed that the attacks targeting activist groups and journalists are not about to lessen.

Moreover, a major rising concern is the fact that these attacks are no longer perpetrated only by the governments of the nation of the victims[3]. Amnesty International Hong Kong revealed that it has been the target of a sophisticated state-sponsored cyber-attack, consistent with those carried out by hostile groups linked to the government of China. This sparks a new debate, and curiously, a new prediction that the most pervasive and sophisticated cyber attacks to target activist groups over the next 5 years, can be perpetrated by a different nation-state.

"In Africa, many civil society actors, activists and journalists face targeted digital threats and cyber-attacks, threatening the security of the people working with them."

2 These categories were: Human Rights, Democracy and Governance, Accountability, Legal and Justice, Media and Gender/LGBTQ.

3 As we saw with the targeted campaign on Amnesty International's office in Hong Kong by state-sponsored hackers from a different State. See : https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

2. Organisations Working to Enhance the Digital Security of Civil Society Actors

Organisation	Country	Activities
AccessNow	USA	Access Now's Digital Security Helpline works with individuals and organisations around the world to keep them safe online. If you're at risk, they can help you improve your digital security practices to keep out of harm's way. If you're already under attack, they provide rapid-response emergency assistance. You can find more info here
Electronic Frontier Foundation (EFF)	USA	EFF is the leading nonprofit organisation defending civil liberties in the digital world. EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. Their Surveillance Self-Defense to protecting you and your friends from online spying. To know more, read the basics to find out how online surveillance works, dive into their tool guides for instructions to installing most secure applications.
Citizen's Lab	Canada	The Citizen Lab is an interdisciplinary laboratory which studies information controls—such as network surveillance and content filtering—that impact the openness and security of the Internet and that pose threats to human rights. Website here
CyberSecurity Non-Profit (CSNP)	USA	CSNP is a non-profit organisation dedicated to promoting cybersecurity awareness and education. Their goal is to make security knowledge and free training accessible, so everyone can learn how to protect themselves and their organisation from cyber threats. Check their resources here
CiviCERT	USA	CiviCERT is a network of Computer Emergency Response Teams (CERTs), Rapid Response teams, and independent Internet Content and Service Providers who help the civil society prevent and address digital security issues. You can find more here.
Co-Creation Hub	Nigeria	CcH is an innovation centre dedicated to accelerating the application of social capital and technology for economic prosperity. Check out their digital security programme here.
Serianu	Kenya Ghana Nigeria Uganda	Serianu is a Pan-African based Cybersecurity and Business consulting firm that enables organisations to extract value from their information assets. They publish the annual Africa Cyber Security Reports. Check out their resources here
HelpDesk of Reporter Without Borders	Germany	Helpdesk is a resource for journalists who want to inform and train themselves about digital security. They provide a free online training program about digital security concepts for journalists, consisting of short videos and regular online consultation. Register for their training here: https://helpdesk.rsf.org/training/
Internews	UK, France, Nairobi, Kenya	Internews empowers people worldwide with the trustworthy, high-quality news and information they need to make informed decisions, participate in their communities, and hold power to account. They publish SaferJourno, a free and open-source curriculum guide for media trainers who teach students, professionals and peers digital safety and online security. Website here
Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG)	US Africa	Internews has developed SAFETAG™, a framework that a digital security expert can use to help organisations identify and prioritise the risks they face and suggest a tightly-focused path to mitigating them. SAFETAG audits serve small scale civil society organisations and independent media houses who have digital security concerns by working with them to identify the risks they face and providing capacity-aware, pragmatic next steps to address them. Check out SAFETAG Audit Framework here

The work of organisations like AccessNow, Electronic Frontier Foundation (EFF), Citizen's Lab, and efforts from groups like RareNET and CiviCERT, who have put themselves at the forefront of protecting human rights defenders globally, could be commended, although much more needs to be done, especially in terms of level of awareness and response to digital threats by target groups in Africa. Also, the West Africa Civil Society Institute (WACSI) believes that technology is a powerful force for social change in West Africa. CSOs' impact can be expanded through better application of technology as a way of creating an efficient and effective environment for them to deliver their critical mandate of promoting sustainable community development. Under the 'Technology for Development' theme from its 2018-2022 strategy, WACSI has initiated actions to bridge the persistent knowledge and capacity gaps that may be hindering CSOs from maximising the benefits of technology.

It is within this context that WACSI, with support from the Open Society Initiative for West Africa (OSIWA), organised a three-day workshop on digital security to provide activists in West Africa with required knowledge, skills and tools to optimise their online security. The workshop enabled participants to network, share experiences, develop and integrate more secure practices and tools in their daily work.

Leonid Volkov, founder of the Internet Protection Society (IPS) and Anthony Suley, a digital security expert, facilitated the workshop. They indicated that digital threats can be harnessed by the following factors:

- Through targeted phishing campaigns and loopholes found within un-updated applications and operating systems within the organisation;
- Configuration flaws on networking devices;
- Insider threats because it is not uncommon to find disgruntled employees or moles who act against the interests of the organisation, collecting and divulging sensitive information for the benefit of a rival or even the government.

It is therefore important to help civil society actors, activists and journalists to identify the strategies and tools they need to secure their personal and organisational digital footprints, or to respond to emergencies and critical threats as they happen.

3. Protecting Organisational and Personal Digital Footprint

Diigital security for any organisation is not a one-off event, and irrespective of the number staff in the organisation, changing habits and retrofitting old systems and policies is difficult and sometimes, expensive. Based on the experience of Co-Creation Hub in addressing digital security needs and making the big changes necessary to protect individuals and organisations, here are some steps civil society actors can take to begin addressing their security needs:

- To change the organisational culture or consciousness on digital security;
- To create policies and a strategy with a budget for digital security and finally,
- To take responsibility for sensitive data every day.

a. Changing cultures: security for any organisation requires willingness and collective effort

The first step to any security strategy is an organisation-wide willingness to embrace secure practices. It involves all staff knowing what is at stake. Staff need to understand that they have a key role to play in safeguarding the security of the organisation and its interests. After understanding their role, they must recognise that digital threats exist and understand the key forms of attacks. CSOs often respond to digital security threats by bringing in a security trainer and/or holding webinars on the basics or on whole new strategies[4]. Though laudable, trainings and webinars simply aren't enough[5] because new threats

4 Josh Levy and Katie Gillum, 'Tackling Digital Security Across Civil Society' , https://ssir.org/articles/entry/tackling_digital_security_across_civil_society. [Accessed 27 September 2019]

5 These guides, trainings, and webinars are explaining the need for encrypted messaging services, secure email, and protected social media accounts are essential.

emerge, hence, the risks to organisations are continually shifting. Thus, trainings should not be a reactive measure. They should constitute a preventive measure.

Organisations are only as secure as their weakest links (usually an individual). To attack an organisation's digital interface, those who follow security best practices are not the target for an attacker, it is those who do not follow these best practices. Therefore, digital security awareness is important for every employee, from frontline staff to the head of the organisation. To address structural vulnerabilities, CSOs need to start thinking about digital security as a capacity-building effort with a multi-stage process, including:

- Understanding the organisation's "threat model"—the adversaries they face, the data they might want, their vulnerabilities and how likely it is for an attack to occur;
- Auditing and assessing technologies (computer systems, servers, applications), processes, and people, with a focus on introducing new cultures and perspectives on dealing with and responding to digital threats and issues, as opposed to simply finding and addressing vulnerabilities;
- Testing staff knowledge and readiness through threat simulation campaigns (ethical hacking), periodic training and update on digital threats, championed by different staff members on a rotational basis.

b. Digital security deserves a strategy and a yearly budget

Regardless of an organisation's sizes, digital security does have some cost implications. As Co-Creation Hub and WACSI noticed in their work, digital security for CSOs is not so much a case of financial might or spending power. It is more about organisational consciousness of the need for it.

In 2017, Serianu (a Kenyan-based security consulting company) revealed in its annual report that cybercrime across Africa reached $3.5 billion in 2017 but 90% of African businesses are operating below the security poverty line (SPL), which is the point below which an organisation cannot defend itself against a cyber-attack. Serianu pegged this line at $1,500. In other words, 90% of African businesses do not devote up to $1,500 to their digital security.

For CSOs in West Africa, Co-Creation Hub's analysis shows that the SPL is around $650, less than half of the cost for businesses. Again, what is interesting in the case of civil society groups is that the SPL is really one of willingness, not money. CSOs don't exactly know what threats they come up against, and consequently, do not do enough to plan for or address them. For example, a CSO in Africa[6] with a shoe-string budget but that understands its risks and commits $150 annually to a security programme is better of, and lives above the SPL, than a CSO able to afford $1,500 for security but has no consciousness, plan or budget for this. ith access to the right platforms and organisations (like AccessNow and EFF), the average CSO in Africa can have a 'fool proof' security programme (and we will make an argument for this on a different article), but first; digital security has to make it to the annual budgets and planning for an organisation.

c. Take responsibility for sensitive data

CSOs are increasingly creating more data every day. That data has great value to third parties who may wish to use these datasets to monitor individuals or gain access to private information. Organisations who capture, disseminate and analyse potentially sensitive data must strengthen their understanding of the technological climate they are wading into, along with their potential liabilities. Establishing internal policies and guidance for staff and volunteers will ensure that technology has the best possible impact while always seeking ways to minimise risk.

In West Africa, CSOs need to take the responsibility of gathering, managing and protecting their data seriously. If they don't, they put their beneficiaries, supporters, and entire institutions at risk. There is a need to secure both organisations' and third-parties' assets - job many CSOs are currently ill-equipped to manage. CSOs must strive to develop capacity to take up increasing responsibility of ensuring the data they handle are safe and secure.

6 Nir Kshetri, 'Cybercrime and Cybersecurity in Africa', *Journal of Global Information Technology Management* 22, no. 2 (3 April 2019): 77–81, https://doi.org/10.1080/1097198X.2019.1603527.

4. The Way Forward

Data and information constitute an asset to any organisation. Civil society generates an enormous amount of datasets that is vital for global development. It is therefore imperative for CSOs, activists to take appropriate measures to secure their digital footprints and datasets. The Global Philanthropy has an estimated $1,5 trillion worth of resources in data and information. A Social Innovation Exchange' survey shows that big foundations are now taking systematic action to counter misinformation. For the human factor can break down almost anything, even the most intelligently designed security system.

The most common types of attack are internal attacks, caused by disgruntled, or angry employees. Thus, organisations need to properly train staff to be able to react when there is a cyber-attack through a well-defined mechanism that was. Such trainings should be organised

"Civil society generates an enormous amount of datasets that is vital for global development. It is therefore imperative for CSOs, activists to take appropriate measures to secure their digital footprints and datasets."

at regular intervals, ideally every quarter.There are lots of activities supported by Hewlett, Knight and others to tackle fake news and threats to democracy. At the continental level, the African philanthropic community should support larger efforts in capacity building at the organisational level. Investing in civil society – its preparedness, digital infrastructure and inclusion in the governance of emerging technologies – is critical for ensuring a fairer, human-centred Fourth Industrial Revolution.

Civil society organisations need strategies and resources that take their value-focused objectives, limited resources and commitment to responsible use of data into account, especially in their work with vulnerable populations. Advocacy groups and humanitarian, development and other non-profit organisations need a broader platform for shared insights on driving and developing responsible data practices. Non-profits and grantee groups should include digital security plans and associated costs in their pitches and proposals. It is both a collective and individual responsibility for all to start or continue to engage in the dialogue about what is at risk leveraging on different opportunities.

"Advocacy groups and humanitarian, development and other non-profit organisations need a broader platform for shared insights on driving and developing responsible data practices."

Conclusion

With new technologies come greater responsibilities – including the responsibility for journalists, activists and human rights defenders to be secured in the digital space. As illustrated, there are associated risks and unintended consequences. To face these risks and concerns about data protection, digital misinformation and ethical use of technologies, there is a need to coordinate information and responses between public, private and non-profit organisations and to provide an appropriate legislative framework[7]. There is also a need for greater participation and partnership in governing how these powerful, emerging technologies shape societies. As we have demonstrated, digital security is not a one-person affair and as such, African human rights defenders need to collaborate, share information that will enable improved detection and prevention of attacks.

7 Laws are always a step behind reality, and this is more evident when attempting to classify and pursue cybercrimes. According to a 2016 report by the African Union Commission (AUC) and the cybersecurity firm Symantec, only 20% of African states currently have the basic legal frameworks in place for countering cybercrime. Thus, the importance of Law professionals being continuously up-to-date on technological advances. Read more here: https://www.symantec.com/content/dam/symantec/docs/reports/cyber-security-trends-report-africa-interactive-en.pdf

WACSI

Strengthening Civil Society

-

WACSI 2019 All Rights Reserved