# Cybersecurity in Kenya: Priorities for 2019

## Introduction

The Kenya ICT Action Network (KICTANet) in partnership with Global Partners Digital (GPD) with the support of the government of the United Kingdom held a well-attended Roundtable meeting themed ***Cybersecurity in Kenya: Priorities for 2019,*** which took place on Tuesday, 19 March 2019 at the Sarova Panafric Hotel in Nairobi.

## Meeting Objective and Expected Outcome

The overall objective of the roundtable was; **to increase local stakeholder awareness of cybersecurity issues, and to identify common cybersecurity priorities for Kenya in 2019**. The discussions also included a broad overview of the current state of play in cybersecurity globally, regionally and in Kenya; while providing space to identify stakeholder common priorities and to make recommendations for the year ahead.

## Context

Cybersecurity continues to be a concern not only for the government, but also is an important issue for private sector companies and groups, the technical community, academia, civil society groups and other non-governmental actors given its enormous implications for information security, critical infrastructure, economic prosperity, public safety as well as their relations with other countries.

From a policy and legal perspective, Kenya has enacted the 2006 ICT Policy, the ICT Master plan, 2014 - 2017 and the National Cybersecurity Strategy, 2014, the Kenya Information and Communications Act, and the Computer Misuse and Cybercrimes Act, 2018. There is also a Senate Data Protection Bill – 2018, a draft National Broadband Strategy 2019, and a draft Data Protection Bill and Policy currently under development. Further, the draft ICT Policy developed in 2016 is yet to be adopted.

Despite this progress, the country continues to experience challenges in the realm of cybersecurity. Key concerns include: third-party misuses or shares of confidential data; malware attacks and disruption of business processes; data breaches; and attacks on IT infrastructure resulting in downtime. The key challenges include among others: insufficient technical, investigation, prosecutorial and judicial capacity of law enforcement agencies; low levels of public awareness on security; outdated laws, policies and strategies; weak internal security practices and standards in key institutions; poor detection and reporting of attacks; and, weak coordination among relevant agencies, industries and institutions.

Across the globe, cybersecurity is gaining traction and countries are taking strides to address the emerging challenges. Measures being adopted include the development of policies, strategies and legislation; establishment of response teams for cybercrimes; formation of multi-agency institutions to promote collaboration; providing funding for cybersecurity programs and initiatives; implementing enhanced security practices and standards; enhancing penalties for cybercrimes; addressing threats to critical infrastructure; investing in workforce capacity building; and, promoting end-user education on cybersecurity.

Kenya therefore needs to develop and promote forward looking and responsive policy and legislative environment with cutting edge strategies, designed to promote confidence and integrity of its information systems. Cybersecurity is everyone's responsibility. Guaranteeing cybersecurity is a role that cannot be left to the government alone, as all relevant stakeholders have a role to play based on their respective mandates. Therefore, the development and implementation of policies, laws and strategies on cybersecurity can only be effective when done through multistakeholder approaches. A multistakeholder approach recognizes the essence of public participation, and is designed to ensure that cyber-policy making processes are open, transparent, inclusive and value-based.

This roundtable provided a platform for discussion, streamlined stakeholder inputs and refined national priorities to ensure Kenya becomes a regional ICT hub.

## Attendees

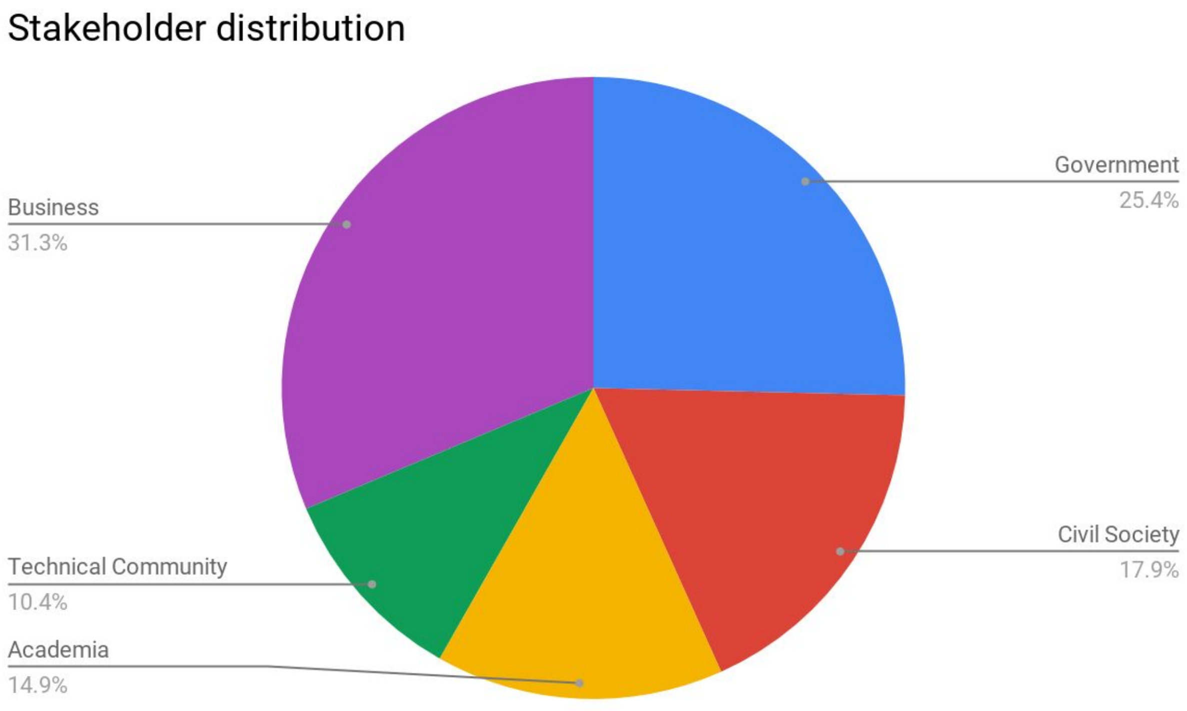
The invitation was targeted to have a balanced stakeholder representation. There were 68 attendants from the three arms of government, including key government agencies and departments, private sector companies and groups, the technical community, academia, civil society groups and other non-state actors.

Classification of the representation is shown on the table below

| **Stakeholder Group** | **Organization** | **No** |
|---|---|---|
| Government | Judiciary Training Institute | 1 |
| | Department of Defence | 2 |
| | Office of the Director of Public Prosecution (ODPP) | 1 |
| | ICT Authority | 2 |
| | Kenya Bureau of Standards | 1 |
| | National Transport and Safety Authority | 1 |
| | Parliament | 2 |
| | US Embassy | 1 |
| | British High Commission | 1 |

| | | |
|---|---|---|
| | Independent Electoral and Boundaries Commission | 2 |
| | Communications Authority of Kenya | 1 |
| | Directorate of Criminal Investigations | 1 |
| | Ministry of ICT | 1 |
| Academia | Kabarak University | 1 |
| | United States international University | 1 |
| | Multimedia University | 1 |
| | KU | 1 |
| | Strathmore University | 2 |
| | Daystar University | 1 |
| | Africa higher education institute | 1 |
| | JKUAT | 2 |
| Civil Society | International Association of Women in Radio and Television | 1 |
| | Paradigm initiative | 1 |
| | KICTANET | 7 |
| | KNCHR | 1 |
| | Amnesty International | 1 |
| | Article 19 | 1 |
| Business | Kiptiness and Odhiambo associates | 4 |
| | Mutemi Sumbi Law | 2 |
| | LawMark Partners LLP | 1 |
| | Serianu | 1 |
| | Huawei | 2 |
| | Credit for Kenya | 1 |
| | Safaricom | 2 |
| | ICANN | 1 |

| | | |
|---|---|---|
| | Oxygen Marketing | 2 |
| | Media force communication | 1 |
| | Credit info Kenya | 1 |
| | Optimal consulting | 1 |
| | Predictive lab | 1 |
| | Lawyers hub | 1 |
| Technical Community | Computer Society of Kenya | 1 |
| | ISACA | 1 |
| | Internet Society | 2 |
| | TESPOK | 2 |
| | Cyberspeak | 1 |
| **TOTAL** | | 67 |



# Meeting outcomes:

The key note speech was given by Hon William Kipsang, Member of Parliament for Marakwet West, and Chairman of the Communication, Informational and Technology committee of National Assembly. He encouraged government security organs to attend such forums to gain knowledge. He urged participants to engage in **public participation** when enacting laws, instead of challenging legislation once it has been passed. He gave an example of the Computer Misuse and Cybersecurity Act of 2018 where a Judge suspended 26 clauses, while such issues could have been resolved earlier. **He also stated the need to operationalized Article 10 of the Kenyan constitution, where a law needs to be enacted on public participation.**

He also **challenged the government to operationalize the draft ICT policy 2016**. He stated that Parliament **Priorities for 2019 were enactment of the Data protection law, and the critical infrastructure law.**

He challenged KICTANET to be a leader on emerging issues to protect the public from cybersecurity threats through sensitization, and advocacy. This will lead to better policies. The MP ended by giving commitment that **Parliament is open to engagement from all stakeholders.**

## Cybersecurity in Kenya - State of Play

The first session gave an overview of Kenya's progress in the implementation of its Cybersecurity Strategy, regional developments in cybersecurity laws and policies, global cybersecurity context and emerging best practice and approaches, and the review process and roadmap of the Cybersecurity Strategy.

It was noted that increase of Internet penetration has led to more cybersecurity related incidences, while there is no increase in protection against cybersecurity risks. The types of attacks and sophistication have increased. The attacks are from global sources. There is a Cybersecurity Strategy in Kenya of 2014, but it needs to be updated through the legislative framework. The new laws on cybersecurity like the Computer Misuse and Cybersecurity Act of 2018 have their flaws, but having the laws in the first place is progress.

Organisations like Safaricom seeks to have confidentiality, integrity, and availability of their systems, therefore they focus on prevention, detection, and appropriate response of cybersecurity attacks. Safaricom noted that education and awareness helps to curb social engineering based cybercrime.

There was concern that Kenya's Penal code and Kenya ICT Act are outdated and are not aligned with modern realities on cybersecurity. It was noted that the Computer misuse and cybercrime Act 2018 was implemented by the Ministry of interior while the Data Protection Bill of 2018 is being championed by the ICT Ministry. This created an overlap, and confusion in implementation. One view for the overlap was that there was interest from one Ministry to control the resources that come with implementing, and operationalizing a new law. There was a view that these laws should be implemented by the same entity. NTSA thought that the state of cybersecurity was divided between those who have suffered cybersecurity attacks, and those who have suffered and don't know. We should look at cybersecurity form a risk perspective because risks are evolving quickly, and there is need to bring lawmakers closer to innovators.

New cybersecurity risk include IoT where system malfunction can have dire consequences, like causing plane accidents. One way for organizations to reduce risks is to train employees.

The CEO of ICT Authority Dr Catherine Getao listed the achievements of government, which are; National Cybersecurity Strategy of 2014, Computer Misuse and Cybercrimes Act, draft ICT Policy 2016, draft National Broadband strategy 2019, and Draft Critical Infrastructure Bill. She noted that the goal of Government in cybersecurity is for citizens to receive quality services without interruption. There is also a draft Public Structure and Safety bill that bill prevent the destruction of public infrastructure.

She noted that Youths need to be trained on cybersecurity. Youth can be indoctrinated, and parents are not able to control the values and norms of children's principles and values consistent with our ways of life. There should also be increased awareness in government of the importance of cybersecurity. It was noted that there were discussion to have a CIRT among infrastructure companies like the Oil Pipeline, Kenya Electricity Generating Company, and Kenya Power.
The National CIRT at CA work in a Multistakeholder fashion.

Process for developing a new National Cybersecurity Strategy is underway, and it will be inclusive. She also emphasised that one important pillars of the Cybersecurity Strategy is capacity. Her view was that the real issue in cybersecurity is common values, and how to impart the values to the society.

On whether government should keep its citizen data with foreign agents, she said data should be held by an entity who can keep the policy, and keep the law. The government should also categorise it's data the way Belgium has, so that we can have four categories of data; person, land and infrastructure, assets, and organizations.

Lawyer Stephen Kiptiness noted that cyberspace is cross border, and it is highly recommended that national legislation should be enforceable in the jurisdictions it seeks to regulate. The bigger question to pose is how practical it is to enforce Laws for cyberspace. This includes the three aspects of right to prosecute, tort (civil wrongs with each other), and contacts (allow legitimacy of contracting each other). On extraterritorial laws (cross border laws), the geographic extent of the law should be considered. A law can only go as far as it is enforceable, and governments rely on mutual legal assistance to prosecute across borders. The principle of mutual assistance helps in cross-border enforcement for crimes that both countries recognize. Government should hold others accountable to secure its data hosted with other agents. Government should also assure its citizens of confidentiality of their data.

It is possible to have specialized courts on cybercrime but budget is the deciding factor.

A judiciary representative from the Judiciary training institute said that it is interested with this discussions to fill the knowledge gap.

## Review of Kenya's National cybersecurity strategies:

William Makatiani, Managing Director Serianu Limited give a presentation on their research; the Cybersecurity Report of 2018 highlighting the cybersecurity challenges in Kenya.

Cybersecurity challenges in Kenya identified were; growing youth population, globalisation, technology adoption and automation, cloud computing, mobile computing, social networking, access to internet, and bring your own device (BYOD.

In the Africa Cybersecurity Report 2018 by Serianu Limited, the following statistics on the state of cybersecurity were shared:

- 90% of Africans operate below cybersecurity poverty line, that is the point below which an organisation cannot effectively protect itself against losses to cyber attackers
- 97% of organisations Spending Spend less than US$10000 on cybersecurity per year. While the budget should be determined by the size of the organisation, and the risk exposure.
- 64% of organisations don't train their employees on cybersecurity at all or only do so when an incident occurs
- 40% of organisations are leveraging on Cloud computing capabilities to improve business operations.
- 83% Board members and Exco are now moving away from generic audit reports and are seeking to understand quantifiable metrics on visibility and exposure for the organisation.
- 83% of orgs manage their cybersecurity in-house.
- 90% of parents don't know the measures to take to protect their children online
- Africa has only 10,000 cybersecurity professionals serving a population of 3 billion.
- Banks ranks highest in cybersecurity preparedness, followed by Sacco, and then government

Makatian felt that Internet of Things (IoT) Security is a stretch on the Africa, and Kenyan market. but it is an emerging issue in the West.  His views was that there are more pressing issues in this market.

A cybersecurity expert was identified as someone who is consistently working on cybersecurity issues, is research driven, and a lifelong student. To bridge the skills gap, Universities needs to allocate funding and train on relevant issues.

The team went through group-work to review Kenya's cybersecurity strategies. The areas of focus were Gaps in the Implementation of the Strategy, common cybersecurity interests and priorities for 2019, and Existing opportunities for interventions.

The matrix below shows the issues that were identified

**Social issues**

| **Issue** | **Solution** |
|---|---|
| Users not aware of cybersecurity issues | Conduct capacity building |
| Uncoordinated response to cybersecurity issues | Encourage multistakeholder participation |
| No national values. | Identify clear set of national values and Implement training and awareness. |
| Lack of cybersecurity expertise | Incorporate cybersecurity training in the education system |

| | |
|---|---|
| Uncoordinated development of cybersecurity frameworks | Proper coordination in development of cybersecurity policies. Create information sharing frameworks. Research and develop evidence based solutions. Use existing frameworks to develop security policies |

**Political issues**

| Issue | Solution |
|---|---|
| Power differential when setting policies. Those with resources have more influence. | Affirmative action to drive inclusivity.<br>Set boundaries between people, and state. |
| Securitization of state, disproportionate use of state resources | Proportionate use of state resources |
| Conflict of interest between stakeholders. | Collaboration. |
| Lack of clarity in handling cybersecurity issues. | Collaboration of relevant entities and develop clarity and policy to manage the process. |

**Environmental issues**

| Issue | Solution |
|---|---|
| Insufficient protection of industrial systems control | Have alert systems to identify intrusion attempts, and challenges on network. |
| Ignorance of cybersecurity issues. | Awareness creation and advocacy. |
| E-waste. | Implement regulations and standards to manage e-waste, type approval |

**Technological issues**

| Issue | Solution |
|---|---|
| Lack if cybersecurity experts. | Research and investment in schools |
| Cost to implement solutions high Licenses are expensive, tools too. | Assign budgets. Find tools alternative tools to handle the same solutions, like open source tools |
| Equipment don’t go through certifications. | Type approval |
| Some tech are not implemented correctly. | Capacity building on technical personnel |

| | |
|---|---|
| No clear guidelines of experts. | Regulate experts |

**Legal issues**

| **Issue** | **Solution** |
|---|---|
| Lack of proper training of legal practitioners. | Offer collaborative training between cybersecurity experts and legal minds. |
| Narrow outlook of cybersecurity issues. | Needs holistic view. |
| Lack of laws. Legal landscape does not evolve as fast as the tech environment. | Update existing laws, and create new ones |
| Few experts in legal profession. | capacity building, and multistakeholderism |
| Egoism between legislature and executive | Improved Diplomacy |
| Legal foundation is adversarial. We have laws but enforcing the is a major challenge. | Consistency on application of the law |

**Economic issues**

| **Issue** | **Solution** |
|---|---|
| Coordination needed between public and private organizations. | Multistakeholderism |
| Lack of funding | Allocate appropriate budget |
| Cyber conversation is driven by economic considerations, and interests of citizens is left behind. | Sensitization on importance of prioritizing cybersecurity issues |

## Opportunities for Multistakeholder Engagement

Gbenga Sesan, Executive Director of Paradigm Initiative took participants through the value of stakeholder engagement in cybersecurity. He gave an example of how multistakeholder action of

- training, and digital engagement roundtable, enabled development of the digital rights and freedom bill in Nigeria.
- joint statement on internet shutdown and responsible Internet use by multiple stakeholders in several countries which have had internet shutdowns have helped in toning down government excesses.
- KICTANET as a leading example of multistakeholderism in East Africa, it provides an opportunity for other regions to learn from the model. Working together through KICTANET has presented opportunities to identify gaps and work towards fixing the issues.

The lessons presented by multistakeholdersim were:

- When hardworking and knowledgeable people, blinded by biases, argue, there can be no winner
- Engagement doesn't mean agreeing at all times. There'll still be lawsuits, call-outs and peace meetings
- No condition is permanent. Stakeholder groups are fluid, with increasing ease of movement by individuals
- There are always those problems everyone agrees on. Start from there. The others will get individual attention
- We can't afford to create a new problem while solving an existing problem. We must respect rights while tackling security challenges

The panel on Multistakeholder engagement sort to get the opportunities for engagement, why all stakeholders should get involved, how governments can benefit from stakeholder engagement in cybersecurity, emerging best practices and lessons, and tangible and SMART things that can be done to improve multistakeholder engagement.

Communication Authority of Kenya (CA) gave an example of the  National CIRT (Computer Incident Response Team) as an example of multistakeholder engagement, and information sharing for the CIRT being a priority for 2019 . Opportunities for engagement includes devices type approval, and sensitizing parents on risks of the cyberspace for their children. CA noted that parents were not aware that children were accessing inappropriate content from parents phones; and parents don't know how to protect their children.

Kenya Alliance of Manufactures (KAM) gave an example of the Court user committee where The judiciary engages with KAM on illicit trade issues. To KAM, Leadership on how you move around teams, and the assumptions you make on interests at play helps in multistakeholder engagement. KAM reiterated that sealing policy and legislative gaps and the need to collaborate would help in curbing cybersecurity.

Cyberspeak identified skills gap as a priority area for 2019.

TESPOK noted that multistakeholderism helps in build trust. The CEO Fioa Asonga divided stakeholder engagement into several groups; consultative (sharing knowledge), discussion (finding decision on way forward), deliberative, and decision making.

## Recommendations, Next Steps and Sustainability

1. Identify groups that can lead on different issues, and ultimately develop a national blueprint.
2. Map different stakeholders, their capabilities and capacity, tools, and interventions they need.
3. Have a dashboard where every stakeholder knows what is going on.
4. What should have been achieved the next time stakeholders meet again? This will avoid cyclic repetition
5. Adopt existing frameworks and nationalize them
6. Get a consultant to map out stakeholders and issues that affect each stakeholder, and develop a zero draft.
7. The patience of walking this journey and fatigue of tagging every stakeholder along is required.
8. Knowledge management and curating lessons learned is required so that there is continuity when individuals leave their roles.

9. Work towards political will to drive this process. KICTANET has a working relationship with different arms of the government, and other stakeholders.
10. Since Judiciary processes takes time, it is important to participate and engage during law creation before the law is enacted. There is also an opportunity to engage and appeal up to six months after a law has been passed.

*This Report was produced by Mwendwa Kivuva, an Associate at KCITANet - www.kictanet.or.ke* | *info@kictanet.or.ke*