KiCTAnet

KENYA ICT ACTION NETWORK

KICTANet's submission to the intersessional meeting, 2-4 December 2019, New York UN Headquarters: 405 East 42nd Street, New York, NY, 10017 EU Delegation: 666 3rd Ave, New York, NY 10017

About KICTANet

The Kenya ICT Action Network (KICTANet) is a multistakeholder policy forum that brings together individuals and organizations interested in, and working on ICT policy and regulation in Kenya. KICTANet's overall objective is to act as a catalyst for reform in the ICT sector and therefore supports national objectives towards ensuring ICT enabled growth and development. Other subsidiary objectives include: improve the engagement on ICT policy processes; provide platforms for policy debates and discussions; engage in policy processes; facilitation of effective dissemination channels; and, enhancing partnerships with individuals and organizations working at the community and around the globe on areas of mutual interest. KICTANet also provides a platform to enhance collaboration among organizations and networks interested in working together to achieve the national aim of ICT enabled growth and development.

Introduction

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. This is due to its enormous implications for information security, critical infrastructure, economic prosperity, public safety as well as their relations with other countries.

The government of Kenya has embraced digital finance and online self-service platforms as an avenue for service delivery. Local banks and financial institutions have been on a mission to introduce various mobile and online financial services. Telecoms companies are competing to offer mobile payments and money transfer services using various products. Micro-finance institutions are offering mobile based loans. In addition, global companies such as Amazon and AliExpress now ship to Kenya, with the latter accepting payments through mobile money platform- mPesa. Other services that can be accessed online and paid for through mobile money platforms include electricity, water, insurance, travel, and examinations (equate the mobile money to the credit card).

However, it is important to note that the continued use of such platforms presents a growing sense of danger on the safety and security of such platforms. The government, and financial services sector including banking and mobile money services remain the top risk areas for the country.

The risks include: malware attacks and disruption of business processes targeting critical mobile and internet banking infrastructure; social engineering aided by the mobile phone, third-party misuses or shares of confidential data; data breaches; and attacks on IT infrastructure resulting in downtime.

Other risks are: 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.

In our work with Global partners Digital, we have seen and agreed that Cybersecurity is everyone's responsibility. Guaranteeing cybersecurity is a role that all relevant stakeholders have to play based on their respective mandates. And 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. Effective stakeholder engagement starts with a clear objective for consultation, followed by the identification of people and organizations with a specific interest in the initiative (*like we are doing now*). And most important, there must be commitment from political leaders in support of cybersecurity. This allows policymakers to understand stakeholders, their roles and divergent interests (including tolerance on divergent views).

Our Story, our lessons learnt

As KICTANet, we have learnt that multistakeholder processes entail:

1. identification of groups that can lead on different issues.
2. Mapping of different stakeholders, their capabilities and capacity, tools, and interventions they need. In the last two years, KICTANet recorded an important partnership with law enforcement who have participated and continued to engage on capacity building areas and to understand the cyberspace.
3. *Using a dashboard where every stakeholder knows what is going on.*
4. Indicators of achievement as well as challenges every time stakeholders meet again during a process. This helps avoid cyclic repetition.
5. Adopt existing frameworks and nationalize them.
6. Mapping out issues that affect each stakeholder, and developing 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 necessary so that there is continuity when individuals leave their roles.
9. Very important to work towards political will to drive a process. KICTANET has a working relationship with different arms of the government, academia, media, legal and other stakeholders.
10. Judiciary processes takes time, and therefore 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.

Recommendations

The effectiveness of the measures will depend on how ICT policies are developed, implemented and progress monitored. The national government and its agencies, in collaboration with all relevant stakeholders, should strive to prioritize cyber security, prepare in advance, develop appropriate policies and practices, build partnerships, implement relevant programs, focus on people and marshal the necessary political will to make cyber security in the country a reality, briefly outlined below as the 6 P’s.

Priorities - All stakeholders should prioritize cyber security. A risk-based approach to cyber security should be encouraged and adopted by all stakeholders. Policy makers should strive to ensure policy making processes are open, inclusive and transparent.

Policies - There is need to implement a comprehensive and coordinated approach to cybersecurity policy development and implementation. The country should endeavor to adopt standards, best practices to realize the full potential of ICTs, and to meet the aspirations and needs of the people

Political Will - Clear and committed leadership coupled with political will is key to achieving the targets. This includes allocating and making resources available for the diverse ICT tasks and coordinating approaches. To ensure robust leadership from government on cybersecurity matters, there is a need to build consensus and clarify the interests, roles and responsibilities of key institutions

Partnerships - Multistakeholder approaches should be adopted, promoted and sustained to ensure broad, open and inclusive participation of all relevant stakeholders drawn from relevant actors within national and county governments, the private sector, civil society, technical communities and academia in the implementation of effective cyber security strategies, including in the coordination of responses and cooperation in information sharing. This should also take into account the diverse roles and responsibilities of the different stakeholder groups without discrimination, in order to promote trust and build confidence. Cybersecurity policies, laws and strategies should be developed through consultative processes that benefit from the collaborative effort and input of these stakeholders given their unique roles, skills, needs and capacities. Key stakeholders should be mapped and convened regularly to share information, strategies and approaches.

Preparation - There is a need to invest in cybersecurity capacity building, including: the training of boards, employees and technical personnel in organizations; relevant personnel within the criminal justice system and law enforcement agencies; and young people within the education system. In addition, it is important for awareness creation for the general public; and, conception and dissemination of tools designed for use by the public to protect themselves. Further, investment in evidence based research on cybersecurity will be critical as part of the early warning systems.

People - At the center of an effective cybersecurity initiative should be people. The measures whether policy, legislative or administrative, should be rights-respecting by design.

Conclusion

Given the complexity of the ICT sector, the desired impact and benefits can only be achieved where the approach of policy development is more inclusive and expertise driven. For policy to be effective, it must be grounded on the engagement with stakeholders (Multistakeholderism). Policy makers therefore, need to recognize the value of inclusive approaches, and commit to them by engaging with more stakeholders and ensuring the diverse views are considered and included. The result will be appropriate, meaningful, holistic and legitimate policy outcomes that deliver dividends to the public. (hope that this OPWG will remain inclusive).

Submission made by Grace Githaiga (@ggithaiga) for KICTANet (@KICTANet).

For more please visit https://www.kictanet.or.ke/?page_id=40115