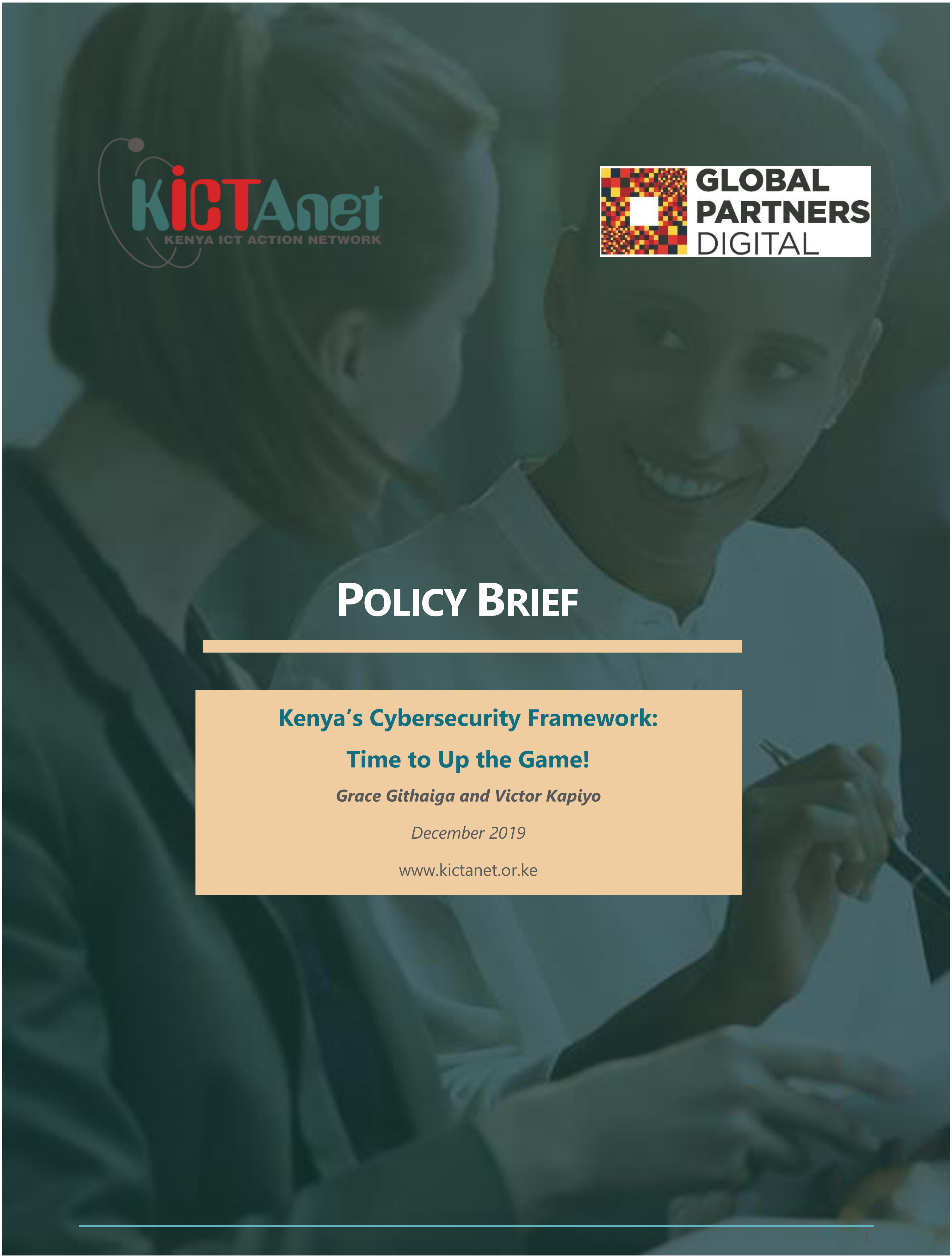

# Policy Brief

## Kenya's Cybersecurity Framework: Time to Up the Game!

*Grace Githaiga and Victor Kapiyo*

*December 2019*

www.kictanet.or.ke

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Cybersecurity is one of the emerging concerns in the ICT sector in Kenya, given the increased adoption of ICT systems across almost every sector. Unfortunately, and even as there is an upward increase in the adoption of ICTs, institutions have not prioritized cybersecurity as a risk. In addition, the country is yet to put in place an appropriate policy, legal and institutional and multistakeholder framework to tackle the emerging cybersecurity threats. This brief, calls for the establishment and implementation of an effective policy, legal and institutional framework to anticipate, detect, respond and combat cyber threats, and build resilience in the country.

## INTRODUCTION

Globally, there is no universally accepted definition of what cybersecurity is. The Freedom Online Coalition defines cybersecurity as "the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure, so as to enhance the security of persons both online and offline". In Kenya, cybersecurity is defined as the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Further, the Kenya Information and Communications Act defines cybersecurity as the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment".

There have been several developments within the ICT sector since Kenya adopted its first National ICT Policy in 2006. And despite increased attention to ICTs in the country over the last decade, cybersecurity threats remain a challenge. This continues because a large section of ICT users in the country still rely on outdated technologies and obsolete systems and applications that are inherently vulnerable.

In addition, the country lacks a comprehensive legal and policy framework; and continues to struggle with limited cybersecurity capacity, including in the coordination of key state and non-state actors on cybersecurity matters. Further, the ever-increasing number of internet enabled devices, and security related concerns around big data, data analytics, artificial intelligence, cyber war or conflict, the internet of things and privacy in a borderless internet remain potential risks areas.

The goal of this policy brief is to provide a snapshot of the current state of policy, legal and institutional framework for cybersecurity in Kenya, with a view to informing future actions by state and non-state actors.

## APPROACH AND METHODOLOGY

The review methodology included a mixed approach. The approach commenced with a desk review of relevant literature including policies, laws, reports and other documents from other jurisdictions. Key informant interviews were conducted with select experts. A consultative meeting was thereafter convened, and focus group discussions were conducted with several representatives from industry, government, civil society, media and academia in March and September 2019. All the information collected was thereafter analysed and forms the basis of this brief.

## STATE OF PLAY

The government of Kenya has embraced digital finance and online self-service platforms as an avenue for service delivery. Some of the key e-government platforms include digital platforms such as the Kenya Revenue Authority (KRA) iTax platform, eCitizen portal, National Transport and Safety Authority (NTSA) Transport Integrated Management System (TIMS), Integrated Financial Management System (IFMIS), Integrated Election Management System (KIEMS), the Integrated Population Registration Services (IPRS), and the controversial National Integrated Identity Management System (NIIMS) (Huduma Namba).

Local banks and financial institutions have been on a mission to introduce various mobile and online financial services. Likewise, telecoms companies are competing to offer mobile payments and money transfer services with products such as M-Pesa, Airtel Money, Pesapal, Mobikash and Mobile Pay. Micro-finance institutions are offering mobile based loans through products such as Tala and Branch. Local and international ride-hailing applications such as Uber, Little Cab, Bolt, Mondo Ride, SWVL and InDriver have gained popularity with users. E-commerce websites such as Jumia, Kilimall, Masoko, Jamboshop, Avechi, Tuskys Online, Naivas Online, ShopIT among others have become a go-to avenue for online purchases.

Further, global companies such as Amazon and AliExpress now ship to Kenya, with the latter accepting payments through mPesa.[1] Other services that can be accessed online and paid for through mobile money platforms include electricity, water, insurance, travel, and examinations. There has also been an increase in innovation hubs within the ICT sector such as iLab, iHub, Nailab, C4DLab and Andela. Global IT firm IBM set up its research lab in Nairobi in 2013,[2] while Microsoft in May 2019, announced plans to establish an Africa Development Centre in Nairobi.[3]

To achieve Vision 2030 goal of Kenya as a regional ICT hub, the ICT sector was expected to contribute directly and indirectly to an additional 1.5% to Kenya's GDP by 2017/2018.[4] The government has continued to gain increased revenue in taxes arising from the growth of mobile payments and internet-enabled products and services.

In the same vein, Kenyans have equally grown accustomed to, and increasingly depend on online services for financial services, commerce, travel, communications, logistics and so on. By October 2019, the NTSA Portal had been visited 334,561,752 times.[5] According to the Central Bank of Kenya (CBK), between the months of January and March 2019, the country recorded 460.113 million mobile payment transactions valued at 1,064.557 billion[6] and a further 1,147,857 million transactions valued at 7,292.45 billion through the Kenya Electronic

[1] AliExpress M-PESA https://www.safaricom.co.ke/personal/m-pesa/do-more-with-m-pesa/aliexpress-m-pesa

[2] IBM opens Nairobi research lab https://www.theeastafrican.co.ke/news/IBM-opens-Nairobi-research-lab/2558-2048120-view-printVersion-e6n7xaz/index.html

[3] Microsoft opens first Africa Development Centre in Kenya and Nigeria https://news.microsoft.com/en-xm/features/furthering-our-investment-in-africa-microsoft-opens-first-africa-development-centre-in-kenya-and-nigeria/

[4] The ICT National Master Plan 2014 - 2017, http://www.ict.go.ke/downloads/THE%20ICT%20NATIONAL%20MASERPLAN%202014-2017.pdf

[5] NTSA Citizen Self-Service Portal TIMS. See: https://tims.ntsa.go.ke/login_csp.jsp

[6] Mobile Payments Statistics, National Payments System, see: https://www.centralbank.go.ke/national-payments-system/mobile-payments/

Payment and Settlement System (KEPSS/RTGS).[7] In August 2019, the bank recorded 151.828 million transactions valued at 368.504 billion shillings.

There is available evidence that the use of digital channels has reduced costs and inefficiencies for providers; provided convenience for users; and, increased access to services to the public. According to a 2016 McKinsey Report,[8] this widespread adoption and use of digital finance has the potential to provide access to financial services for 1.6 billion people in emerging economies; increase the GDPs of all emerging economies by 6 percent, or a total of $3.7 trillion, by 2025. This would allow governments to save $110 billion per year by reducing leakage in spending and tax revenue.

Nonetheless, 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. In fact, Kenya loses millions of shillings daily due to weak cybersecurity. In 2017, the Kenya Revenue Authority is reported to have lost 4 billion shillings ($39 million) in an elaborate hacking scheme, while the National Youth Service lost 1.8 billion shillings ($17 million) in 2016.[9] In addition, in June 2019, critical government websites including those of the National Youth Service (NYS), Integrated Financial Management System (IFMIS), Judicial Service Commission (JSC), the Immigration Department, Kenya Meat Commission, Petroleum Ministry and the ICT Authority among others were defaced by an Indonesian hacker group, the Kurd Electronic team.[10] In 2017, the Communications Authority of Kenya's website suffered an attack by AnonPlus.[11] In 2013, more than 100 government websites were defaced.[12] Given these attacks, it would appear that the rapid digitalisation strategy by government institutions is being implemented without adequate appreciation or awareness of the apparent risks or measures to ensure information security.

Reports from Kenya's Cybercrime Unit indicate that the country lost 16.9 billion shillings ($165 million) through hacking in 2016.[13] According to a report by Serianu[14], this figure stood at $175 million[15] and by 2018, the cost of cybercrime in the country had risen by 68.5% to $295 million.[16] In the region, the estimated cost of cybercrime in 2017 was $99 million in Tanzania, $67 million in Uganda and $3.5 billion in Africa.[17]

It is important to note that the government, and financial services sector including banking and mobile money services remain the top risk areas for the country, followed by betting sites, e-commerce, hospitality and retail services. The common types of

[7] KEPSS/RTGS Statistics, National Payments System, Central Bank of Kenya, see: https://www.centralbank.go.ke/national-payments-system/kepss-rtgs/

[8] Digital Finance For All: Powering Inclusive Growth In Emerging Economies, McKinsey Global Institute, September 2016. See: http://www.mckinsey.com/~/media/McKinsey/Global%20Themes/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.ashx

[9] Sh1.8bn lost in NYS scam, lawmakers told, Daily Nation, 30 September 2016. See: http://www.nation.co.ke/news/money-lost-in-NYS-scam/1056-3399716-cbfkmcz/index.html

[10] NYS and IFMIS among government websites hacked https://www.businessdailyafrica.com/news/-NYS-and-IFMIS-among-government-website/539546-5143440-kpf08m/index.html

[11] Kenyan government official websites hacked and defaced https://nairobinews.nation.co.ke/news/kenyan-government-websites-hacked

[12] Inside the mind of a hacker https://mobile.nation.co.ke/lifestyle/Inside-the-world-of-a-cybercriminal/1950774-3854410-e6f9e7z/index.html

[13] Kenya Revenue Authority 'lost $39m to hacker', BBC News. See: http://www.bbc.com/news/world-africa-39351172

[14] Serianu is a Pan-African based Cybersecurity and Business consulting firm that enables organisations to extract value from their information assets.

[15] Kenya Cybersecurity Report, Serianu. See: http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf

[16] Kenya Cybersecurity Report, Serianu. See: https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

[17] Africa Cybersecurity Report 2017, Serianu https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

attacks recorded in Kenya include: social engineering of mobile money; use of malware and account personifications; malware targeting critical mobile and internet banking infrastructure; online scams on E-commerce platforms; ATM card skimming and identity theft. Others include organized cybercrimes, ransomware, cyberterrorism and attacks from the dark web.[18]

These are happening despite Kenya being home to 1,700 certified cyber professionals, which according to Serianu, shows weaknesses in the inability of organizations to have adequate cybersecurity teams and strategies and to match their needs with skilled personnel. Likewise, there are few institutions of higher learning in the country offering cybersecurity related training or certification programmes.

It is worth noting that cyber-attacks evolve faster than cyber-defences in frequency, scope and sophistication. The surge of attacks is attributed to a number of factors. These include: insufficient technical training of employees; increase in the number of home grown cyber criminals in Kenya; low level of awareness and insufficient training of law enforcement including the prosecution and the judiciary on cybersecurity. Further, the use of free online content management systems; failure to install system updates, patches and firewalls; and the sale and distribution by service providers of network routers with common default passwords are apparent lapses that can be avoided.

Others are low levels of security awareness amongst the public; lack of practical regulatory guidance from industry regulators and government; and poor anticipation, detection, response and management of attacks as it takes 260 days to detect an attack in a typical organization. Still, there is poor reporting of attacks as 91% of the cases go unreported; weak investigation and prosecution of cybercrimes as only 2.9% of the reported cases are prosecuted. There is also poor recovery and business continuity preparation; poor cyber hygiene culture among the public; and poor prioritization of cybersecurity risk by corporate entities.[19] Also, there is a lack of situational awareness in the implementation of cybersecurity measures, in particular, the failure to recognise cultural experiences, behaviours and practices of the public, with regard to safety and security.

This state of affairs raises fundamental questions on the effectiveness of the existing policy, legal and institutional framework to address the cybersecurity challenges that the country is experiencing.

## POLICY ENVIRONMENT

Kenya's ICT Policy which came into effect in 2006, can be credited for providing the overall direction for the creation of an enabling environment for ICT growth and usage in Kenya. The mission of the policy is to improve the livelihoods of Kenyans "by ensuring the availability of accessible, efficient, reliable and affordable ICT services".

In regard to cybersecurity, the Policy called for the establishment of an adequate legal framework and capacity to deal with national security, network security, privacy, cybercrime and terrorism; and to establish mechanisms for international cooperation to combat cross-border crimes.

Other measures included the development of an e-security structure in collaboration with the relevant institutions; the development regulations to ensure

[18] AMADEUS hosts East Africa's first Travel Cyber Security Forum, Amadeus, May 2017. See: http://amadeusafricablog.com/amadeus-hosts-east-africas-first-travel-cyber-security-forum/

[19] Africa Cybersecurity Report 2017, Serianu https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

telecommunication infrastructure, and networks that are robust and resilient. Further, that they have adequate security, redundancy and backup arrangements. The policy also stated that the Government would create statutory obligations of telecommunications service providers to assist law enforcement in executing legal intercept pursuant to the security needs of the country. The policy tasked the National Communications Secretariat (NCS) as the policy advisory arm of government, while recognizing the roles of civil society, investors and operators, the Communications Authority, development partners, professional bodies and consumers and users.

This 2006 ICT policy has been robustly implemented by successive governments. Perhaps this is evident in the growth and uptake of ICTs and the increase in mobile subscriptions as well as internet usage. This has risen from 3 million and 1 million in 2004, to 39.1 million and 26.6 million in 2017,[20] and to 46.63 million by September 2018.[21]

Other notable results include the adoption of the National ICT Masterplan, National Cybersecurity Strategy, revisions to the Kenya Information and Communication Act, and draft ICT Policy 2016 and Computer Misuse and Cybercrimes Act 2018. Nonetheless, this policy despite being the anchor policy, is outdated and has since been overtaken by time given the number of developments that have taken place within the ICT sector since it was developed.

In recognition of these gaps, Kenya developed in 2014, a National Cybersecurity Strategy[22] to guide its responses to the increasing threats brought about by the growth in use of ICTs. The strategy clearly defined Kenya's cybersecurity vision, goals, and objectives to secure the nation's cyberspace, while continuing to promote the use of ICT to enable Kenya's economic growth. The four goals of the Strategy included to: enhance the nation's cybersecurity posture; build national capability; foster information sharing and collaboration; and, provide national leadership.

The Strategy proposed a number of measures including: creating an overarching government cybersecurity policy outlining the roles, responsibilities, and authorities of different agencies; establishment of a cybersecurity regulatory body to define cybersecurity regulations; definition and identification of cyber critical infrastructure across the public and private sectors.

Other measures included the establishment of sector-specific baseline cybersecurity protection criteria and requirements; document government standards and guidelines for government systems and electronic transactions; the need for public and private sector cybersecurity compliance reporting to regulators; and, to develop a specific cybercrime penal code. The Strategy has since lapsed, and was hardly implemented.

However, a notable outcome was the Computer Misuse and Cybercrimes Act, 2018, which the High Court in May 2018 suspended 26 of its provisions for contravening the constitution.[23] The Communication Authority has continued to oversee and coordinate cybersecurity functions, including the National KE-CIRT/CC.

[20] Third Quarter Sector Statistics Report For The Financial Year 2016/2017, Communications Authority, See: http://www.ca.go.ke/images/downloads/STATISTICS/SECTOR%20STATISTICS%20REPORT%20Q3%20FY%202016-2017.pdf

[21] First Quarter Sector Statistics Report For The Financial Year 2018/2019, Communications Authority, See: https://ca.go.ke/wp-content/uploads/2018/12/Sector-Statistics-Report-Q1-2018-2019.pdf

[22] National Cybersecurity Strategy 2014, Ministry of ICT, Republic of Kenya. See: http://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf

[23] Sections of Kenya's Computer Misuse and Cybercrimes Act, 2018 Temporarily Suspended, CIPESA https://cipesa.org/2018/05/sections-of-kenyas-computer-misuse-and-cybercrimes-act-2018-temporarily-suspended/

The main purpose of the National ICT Master Plan 2014 - 2018[24] was to restate the government's commitment to take advantage of the potential of ICTs to achieve the country's national agenda. It replaced the Connected Kenya Plan and is founded on Vision 2030 and its Medium-Term Plans. The vision of this Master Plan is "Kenya as a regional ICT hub and a globally competitive digital economy" with the guiding principles being: partnership; equity and non-discrimination; technology neutrality; environmental protection and conservation; good governance; and incentivizing.

The plan, lays the roadmap for transitioning Kenya to a knowledge society and aims to position the country as a regional ICT hub. This is through developing quality ICT infrastructure, developing integrated and secure information infrastructure and developing a critical mass of high-end ICT human capital.

In order to enhance data access and protection, the Plan calls for: the development and institutionalisation of a legal framework to enable data and information sharing across Governments (Regional, National, and County), citizens, and Ministries, Departments and Agencies (MDA's); development and institutionalization of a middleware platform to enable secure data and information access; and, the development of a cybersecurity policy. This is in light of the vision of increasing and strategically implementing "one-stop, non-stop e-government services" across the entire public sector.

The eCitizen platform launched in 2014, had by June 2016 registered 1.7 million persons, processed over 2.4 million applications and collected 4.2 billion shillings in revenue.[25] So far, the country is yet to develop a standalone cybersecurity policy or adopt a comprehensive ICT policy. Nonetheless, the Data Protection Policy 2019 and the Data Protection Act 2019 have since been adopted.

In June 2016, the draft ICT Policy was published,[26] which called for the privacy and security of the person to be paramount in the development of ICTs. The Policy dedicates its Chapter 15 to cybersecurity and obligates the national government to promote confidence and security in the use of ICTs, and to put in place appropriate legal measures, organizational structures, capacity building programmes and network cooperation. It also recognizes network security and reliability, national security, information security and child online protection as priorities.

Moreover, it proposed the establishment of a National Cyber Security Agency to among others protect systems, detect, prevent and manage cyber risks and internet-based crimes. Whereas the proposals in the draft policy are useful, it is yet to be adopted three years since its publication.

In August 2017, the Central Bank of Kenya (CBK) released a Guidance Note on Cybersecurity for the Banking Sector,[27] referenced via its mandate under Section 33(4)[28] of the Banking Act. The Guidance Note outlines the minimum requirements that banking institutions should adopt to develop

[24] National ICT Master Plan 2014 - 2017, Ministry of ICT, Republic of Kenya. See: http://icta.go.ke/pdf/THE%20NATIONAL%20ICT%20MASTERPLAN%202017.pdf

[25] Okuttah Mark, Wananchi to pay for more public services electronically, June 9 2016, Daily Nation. See: http://www.nation.co.ke/news/Wananchi-to-pay-for-more-public-services-electronically/1056-3240918-8deva4z/index.html

[26] Draft National ICT Policy 2016 http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf

[27] Guidance Note on Cybersecurity for the Banking Sector, Central Bank of Kenya, August 2017. See: https://www.centralbank.go.ke/uploads/banking_circulars/634077191_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf

[28] The provision empowers the CBK to issue Guidance Notes to be adhered to by institutions in order to maintain a stable and efficient banking system.

effective cybersecurity governance and risk management frameworks.

The Note requires the elevation of cyber risk to the board level and provides roles for the Board of Directors, Senior Management, while introducing the role of the Chief Information Security Officer. It also requires regular independent cyber threat assessment and testing; implementation of guidelines on outsourcing; implementation of IT security awareness training; and cybersecurity incident reporting within 24 hours and on a quarterly basis. The institutions were also required to review regularly and submit their revised Cybersecurity Policy, strategies and frameworks to CBK by November 30, 2017.

The Guidance Note, highlights the risk that could emanate from the prevalent trend of Institutions rapidly expanding their reliance on outsourcing, cloud providers and other services to save time and reduce operation costs. While the Guidance Note provides minimum requirements to address key cybersecurity issues, its limitation is that it is only applicable to the banking sector. The guidelines could be beneficial to other sectors if a similar instrument were adopted at the national level or by relevant sector regulators.

Moreover, standards for IT goods and services, including systems, safeguards and inspections are necessary to address risk factors and prevent compromise, including in the supply chain. It is important to ensure supply chain integrity given the ubiquitous potential for inserting trapdoors, backdoors, and surveillance mechanisms in hardware or software.[29] The Kenya Bureau of Standards (KEBS) Information technology Security Techniques Guidelines for Cybersecurity (KS ISO IEC 27032) is a notable effort in this regard.[30] Since there is no requirement to adopt or comply with the standards, it is not clear how many organizations are aware of the standard, or are compliant with it.

In May 2019, the government launched the Digital Economy Blueprint[31] which embodies the government's strategy towards the realisation of a successful and sustainable digital economy. It is also developed as part of the Smart Africa Initiative[32] where it is expected to be replicated as the blueprint for Africa. The blueprint identifies cybersecurity as an enabler, stating that the "protection of the integrity of electronic and digital systems is a paramount concern in a digitally enabled economy."

Further, it highlights cybersecurity as a cross-cutting issue critical for the development of the digital economy. In order to foster confidence and trust and security of the digital economy, it prioritises data security, privacy, and child online safety. Moreover, it proposes the development of legal, regulatory and institutional frameworks to ensure data security. The blueprint is promising and it remains to be seen how it shall be implemented by the government moving forward.

A notable challenge with the policy making processes relating to some of the documents discussed above is that they are largely not well coordinated or implemented in full. Further, save for the draft ICT Policy 2016 process which was quite participatory, information relating to other processes

[29] Theodore H. Moran, Dealing with Cybersecurity Threats Posed by Globalized Information Technology Suppliers, Policy Brief, Peterson Institute for International Economics, May 2013, See: https://piie.com/sites/default/files/publications/pb/pb13-11.pdf

[30] Kenya Bureau of Standards (KEBS) Information technology Security Techniques Guidelines for Cybersecurity (KS ISO IEC 27032). See: https://webstore.kebs.org/index.php?route=product/product&product_id=10503

[31] Digital Economy Blueprint, Ministry of ICT http://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf

[32]Kenya To Develop A Digital Economy Blueprint For Africa http://www.ict.go.ke/kenya-to-develop-a-digital-economy-blueprint-for-africa/

or the substantive aspects were not widely available or accessible to relevant stakeholders.

# LEGAL FRAMEWORKS

Kenya's Constitution provides for a comprehensive Bill of rights in its Chapter 4. The rights and fundamental freedoms provided for include: equality and freedom from discrimination; human dignity; freedom and security of the person; privacy; freedom of conscience, religion and belief; freedom of expression; freedom of the media; and access to information. Others are freedom of association; assembly, demonstration, picketing and petition; political rights; property; labour relations; economic and social rights; consumer rights; fair administrative action; access to justice and so on.

From the foregoing, it is important to note that the implementation of cybersecurity laws, policies and measures have an impact on these human rights. Therefore, while often overlooked, the protection of human rights remains central to cybersecurity.

The Kenya Information and Communication Act[33] is the main framework law regulating the ICT sector. It defines cybersecurity and provides for the functions of the Commission in relation to electronic transactions. It grants the Authority power under section 83C(2) to make regulations with respect to cybersecurity, which have not been developed. The Act also provides for: consumer protection, responsibilities of service providers and defines a number of cybercrimes. The cybercrimes addressed include: improper use of systems, alteration of messages, interception and disclosure, electronic fraud, and tampering with computer source documents among others. The Act also provides for a Public Key Infrastructure (PKI) framework[34] as a means of securing online transactions.

In 2014, a draft Cybercrime and Computer Related Crimes Bill 2014[35] was proposed by the Office of the Director of Public Prosecutions (ODPP) in response to the increasing cases of cybercrime and also to address the deficiencies of the current regime.[36] The controversial Computer and Cybercrimes Bill, 2017 was in May 2018, assented into law as the Computer Misuse and Cyber Crimes Act, 2018. The objects of the Act are to protect the confidentiality and integrity of computer systems, prevent the unlawful use of computer systems, facilitate the detection, investigation, prosecution and punishment of cybercrimes and to facilitate international co-operation in dealing with computer and cybercrime matters.

The Act failed to provide a robust framework to address the gaps in cybersecurity measures in the country. The law placed a lot of emphasis on the creation of cybercrimes, and their penalties as opposed to putting in place comprehensive measures to ensure cybersecurity.

Where it succeeded, was in violating the Bill of Rights, leading to the suspension of 26 of its provisions for violating, infringing and threatening

[33] The Kenya Information And Communications Act Chapter. 411A. http://ca.go.ke/images//downloads/sector_legislation/Kenya%20Information%20Communications%20Act.pdf

[34] http://www.govca.go.ke/

[35] Kenya: Cybercrime and Computer Related Crimes Bill. http://www.article19.org/data/files/medialibrary/37652/Kenya-Cybercrime-Bill-129072014-BB.pdf

[36] Kenya creates special cyber-crime unit http://www.itnewsafrica.com/2014/01/kenya-creates-special-cyber-crime-unit/

fundamental freedoms in the Constitution of Kenya, 2010[37] through a constitutional Petition.[38]

Be that as it may, the provisions of the law, despite having strong sanctions failed to raise the cost for attackers or make the attacks less difficult to execute, and as such may not impede crime. More importantly, it appeared to focus more on offences, as opposed to establishing a multi-stakeholder approach through effective frameworks and institutions to anticipate and counter attacks, promote standards and cyber hygiene.

The country is in the process of implementing an appropriate legal and policy framework for the protection of privacy. In fact, the Privacy and Data Protection Bill was first developed in 2012, and in November 2019, the Data Protection Act, 2019 was adopted after the consolidation of two bills from both the Senate and the National Assembly. While it was laudable that each of the houses of Parliament had initiated separate bills on privacy and data protection, it was concerning that the parallel approach had led to confusion of stakeholders and a battle for supremacy over which of the bills would be enacted.

The continued absence of a data protection law since 2012 was worrying given the increased uptake of online services and the widespread collection and processing of the personal information of the public by various players without sufficient guarantees as to the security of the information. The implementation of the Data Protection Act, 2019, will be critical.

Regionally, Kenya despite being widely known as an ICT hub, is yet to ratify or sign the African Union Convention on Cybersecurity and Personal Data Protection which was adopted in June 2014.[39] The Convention calls upon State Parties to establish measures to ensure the: security of electronic transactions; adoption of legislation for the protection of personal data; establishment of national personal data protection authorities; development in collaboration with stakeholders, of a national cybersecurity policy and strategies for its implementation; and development of legislation on cybercrime that is rights respecting.

In addition, the establishment or designation of national authorities to act on cybersecurity; protection of critical infrastructure; promotion of a culture of cybersecurity; promotion of public-private partnership on cybersecurity; and the development of capacity and training, among others. Kenya is not a signatory of the Budapest Convention on Cybercrime, which provides a framework for cooperation on cybercrime.

# INSTITUTIONAL ARRANGEMENTS

An effective institutional framework is key to ensure cybersecurity in any country. There ought to be clear leadership, coordinated and multistakeholder approaches, commitment of the relevant institutions, accountability, roles and responsibilities, and transparency in operations. Further, there should be open participation of all relevant stakeholders drawn from academia, business, civil society, government

[37] Justice Chacha Mwita Suspends 26 Sections of the Computer Misuse and Cybercrimes Act. https://www.blog.bake.co.ke/2018/05/29/justice-chacha-mwita-suspends-26-sections-of-the-computer-misuse-and-cybercrimes-act/

[38] Bloggers Association of Kenya (Bake) v Attorney General & 5 others [2018] eKLR http://kenyalaw.org/caselaw/cases/view/159286/

[39] African Union Convention on Cyber Security and Personal Data Protection http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

and the technical community. The country is yet to achieve this.

The mandate of the Communications Authority with respect to cybersecurity is fairly limited. Despite this, it has been able to establish a national Computer Incident Response Team (CIRT). The National KE-CIRT/CC[40] which has benefitted from the support of the ITU,[41] is tasked with the responsibility of monitoring and responding to cybersecurity incidents and work in partnership with the relevant bodies at national, regional and global level.

Its other tasks include: provision of advice on cybersecurity; act as the country's focal point for information for security matters; collect and distribute technical information on computer security incidents; conduct research on computer security; build capacity in information security; awareness creation; and assist in the development of a National Public Key Infrastructure (NPKI). The CIRT-CC has been able to establish collaborative mechanisms through formation of sectors CIRTs, and has identified critical infrastructure such as in the telecommunications, utilities, energy, finance and education sectors that needs to be secured.

Nonetheless, given the increasing cybersecurity incidents, the technical capacity of the CIRT-CC to enable it effectively deal with such incidents remains weak. In addition, the CIRT appears to be crippled given its few experts, minimal resources, its ineffective coordination of cybersecurity incidents and poor engagement with key stakeholders. Additionally, the public negates the noble intentions behind its establishment, while its leadership and membership remains unclear, and so is whether the team actually meets.

Also, there has not been significant efforts and plans to promote public awareness on online safety, save for child safety, or have more robust engagement with service providers to enforce minimum standards or best practices for ensuring cybersecurity. Moreover, the Authority has not developed any regulations on cybersecurity as anticipated under section 83(C)(2) of the Kenya Information and Communications Act. It is likely that the absence of guidance from the sector regulator, contributed to the decision of the Central Bank to put in place Guidelines on cybersecurity for banks.

The Information Communication and Technology Authority (ICTA) was established in 2013, taking over the functions of Government Information Technology Services (GITS), Directorate of e-Government (DeG), and the Kenya ICT Board (KICTB). In its Strategic Plan 2013 - 2018,[42] the Authority recognizes its central role in ensuring the effective coordination of information security across government.

The key objectives include strengthening information security frameworks, functions, capacity, risk management, infrastructure appraisal and the implementation of the Cyber Security Master Plan and Strategy. The Authority developed an Information Security Standard in 2016, which is due for review.[43] The Authority has overseen the roll-out of and training of 22 million young people under the Digital Literacy Programme,[44] and the construction of 9,000 kilometres of the National Fibre-Optic Backbone (NOFBI)[45] against a 50,000 kilometre target.

The Authority has convened the Connected Kenya Summit, an exclusive event which if it were more

[40] National KE-CIRT/CC http://www.ke-cirt.go.ke/

[41] CA to receive ITU Technical Support to Fight Cybercrime http://www.ca.go.ke/index.php/what-we-do/94-news/334-ca-to-receive-itu-technical-support-to-fight-cybercrime

[42] ICTA Strategic Plan 2013 – 2018 http://icta.go.ke/pdf/ICT%20Authority%20Strategic%20Plan.pdf

[43] Information Security Standard http://icta.go.ke/standards/information-security-standard-2/

[44] Digital Literacy Programme http://icta.go.ke/digischool/

[45] National Optic Fibre Backbone (NOFBI) http://icta.go.ke/national-optic-fibre-backbone-nofbi/

open, could be a useful platform for stakeholder engagement on cybersecurity matters. Further, the ability of the Authority to collaborate with key stakeholders, and more so with county governments is critical to the execution of its functions. In addition, the Authority was a victim of an attack on its website in June 2019[46] and while it was able to recover, the incident points to the sheer challenge faced even by the institutions charged with the responsibility to safeguard others, of guaranteeing cybersecurity.

The National Communications Secretariat has a policy making role with regards to cybersecurity policy in line with its mandate under Section 84(2) of Kenya Information and Communications Act. The Ministry of ICT is yet to implement the National ICT Policy 2016 or direct the development of a national cybersecurity policy.

The Office of the Director of Public Prosecutions (ODPP) in 2014 established a cybersecurity department in order to streamline the prosecution of cyber criminals.[47] However, successful prosecution of cyber-related cases remain low, owing to capacity gaps not only at the prosecution level, but also at the investigative and judicial levels. Likewise, a National Cyber Command Centre (NC3) has been established by various state security agencies.[48] Its current roles and functions have not been made public and it remains to be seen how this body will work towards ensuring cybersecurity.

The National Computer and Cybercrimes Coordination Committee established under the Computer Misuse and Cybercrimes Act, 2018 comprises of only government actors, which reflects poorly on the need to embrace multistakeholder approaches on cybersecurity matters. The failure of Parliament to adopt a multistakeholder approach as proposed by KICTANet, the domicile of the Committee within the Ministry of Interior and Coordination of National Government as opposed to the Ministry of ICT, further fuels the perception that cybersecurity is being seen as a purely national security issue, and therefore exclusive to security agencies, if recent developments are anything to go by.

This could affect the ability of the Committee to effectively coordinate with stakeholders on cybersecurity matters, and for the country to implement a comprehensive national strategy to ensure cybersecurity. In addition, it reflects a now common weakness of the relevant institutions responsible for articulating or implementing national cybersecurity strategies and policies which have failed to adequately engage with key stakeholders.

# CONCLUSION AND RECOMMENDATIONS

Kenya's global competitiveness and leadership in the region including as an ICT hub will depend on its ability to deploy ICTs in all aspects and sectors of its economy. Further, internet penetration and the adoption of ICTs has increased in the country, leading to more sophisticated cybersecurity related incidents. However, these developments have not been matched with a corresponding increase in vigilance, protection and responses against cybersecurity risks.

[46] Kenyan government official websites hacked and defaced. https://nairobinews.nation.co.ke/news/kenyan-government-websites-hacked

[47] Kenya creates special cyber-crime unit. http://www.itnewsafrica.com/2014/01/kenya-creates-special-cyber-crime-unit/

[48] New website to help curb online crimes in Kenya https://www.nation.co.ke/news/New-website-to-help-curb-online-crimes/1056-4266396-11mps90z/index.html

Accordingly, building confidence in the use of ICTs requires the acknowledgement by all stakeholders that cybersecurity is a shared responsibility. Policies and strategies alone will not guarantee the desired outcomes. The effectiveness of the measures will depend on how ICT policies are developed, implemented and progressively monitored.

The national government and its agencies, in collaboration with all relevant stakeholders, should strive to prioritize cybersecurity, prepare in advance, develop appropriate policies and practices, build partnerships, implement relevant programmes, focus on people and marshal the necessary political will to make cybersecurity in the country a reality. These are briefly outlined below as the 6 P's.

## Priorities

All stakeholders should prioritise cybersecurity and adopt a proactive approach when dealing with cybersecurity matters. Thought leadership, especially within government is critical. Also, a holistic and risk-based approach to cybersecurity should be encouraged and adopted by all stakeholders. The current gaps in the policy, legislative, administrative and institutional levels should be prioritised for action.

Policy makers should strive to ensure policy making processes are open, inclusive and transparent. Also, the capacity of the National CIRT should be enhanced, coupled with the establishment of government and industry or sector-based CIRTs and points of contact to ensure coordinated incident responses. Additionally, all stakeholders should budget for, allocate sufficient funds and invest in enhancing their cybersecurity.

## Policies

There is a need to implement a comprehensive and coordinated approach to cybersecurity policy development and implementation. The country should endeavour to adopt standards, best practices to realize the full potential of ICTs, and to meet the aspirations and needs of the people of Kenya. The government should review, revise and operationalize the draft ICT Policy 2016 and adopt the Data Protection Policy. In the same vein, revise the now outdated National Cybersecurity Strategy 2014 and the National ICT Master Plan 2014 - 2017.

Policy gaps in key areas including: fostering creativity and artistic expression; infrastructure sharing policy; industry code of practice; information sharing; network integrity, trust, security and e-commerce should be addressed. There is also need to harmonise policies on energy, roads and ICT, as appropriate with provisions for categorization of ICT services and the protection of critical ICT infrastructure.

Legal gaps in such areas as data protection, cybersecurity, intermediary liability, coordination of cybersecurity, public procurement, information sharing, documentation and records disposal should be addressed. The implementation of the Data Protection Act, 2019 should be fast-tracked and the Computer and Cybercrimes Act, 2018 reviewed to ensure it respects human rights and the constitution. It should also meet international best practice.

Likewise, the relevant provisions of the Penal Code and the Evidence Act should be updated to incorporate forensic standards, social engineering, organized crime, intermediary liability, search and seizure among others. The development of institutional policies should be encouraged across all sectors.

Further, regulatory guidance for key sectors is essential to promote risk-based approaches; cyber incident reporting; adoption of standards and best practices; capacity building and coordination. More importantly, policies and legislation are only useful if implemented. Therefore, efforts should also be put in place to not only implement the policies and laws, but to also monitor the process of their implementation.

## 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 such as the Presidency, the Ministry of ICT, the Ministry of Interior and Coordination of National Government, the Department of Defence, the Communications Authority, and the ICT Authority. Accordingly, designate the overall body to provide leadership on cybersecurity matters at the highest level.

Further, the current government-only National Computer and Cybercrimes Committee should be reformed to be the National Cybersecurity Agency. The reforms should also ensure it is independent, representative, multi-stakeholder-based and the designated focal-point responsible for advising and coordinating the implementation of all cybersecurity policies, responses and strategies.

Moreover, cybersecurity responses should not be treated as secret national security matters, that often lack transparency, oversight and accountability, and are not open to public participation or scrutiny. Policy makers need to understand and appreciate that cybersecurity is a shared responsibility, and thus, everyone's duty. As such, no single stakeholder can have the monopoly of ideas or solutions.

## Partnerships

The silo approach should be avoided in the development and implementation of cybersecurity measures, as systems and responses are only as strong as the weakest links. Therefore, 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 cybersecurity strategies.

This should also apply in the coordination of responses and cooperation in information sharing. In addition, it should take into account the diverse roles and responsibilities of the different stakeholder groups without discrimination, in order to promote trust and build confidence. There is need for the establishment of more CIRTs, and the promotion of greater collaboration among them, not only locally, but also regionally and globally.

Cybersecurity policies, laws and strategies should be developed through consultative processes that benefit from the collaborative effort, expertise and input of these stakeholders given their unique roles, skills, needs and capacities. Key stakeholders should be mapped and convened regularly by the government cybersecurity focal point, to create opportunities for dialogue, information sharing, strategy development and the review of approaches. Further, special attention needs to be paid to the role of ICT service providers, while also leveraging on Public Private Partnerships (PPPs) to strengthen cybersecurity.

Moreover, partnerships and cooperation should be extended to the regional level at the East African Community and the African Union. Other platforms that can be useful include the Freedom Online Coalition, the International Telecommunication Union (ITU), the Global Forum on Cyber Expertise (GFCE), the UN Open Ended Working Group (OEWG) on cybersecurity, the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security and the United Nations General Assembly, in which Kenya actively participates.

## 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 including judicial officers, and law enforcement agencies; and young people within the education system at primary, secondary and tertiary levels. 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.

There is also need to ensure that there are robust efforts applied in the prediction, anticipation, detection, response and management of cybersecurity risks by all stakeholders. In this regard, investment in enhancing cybersecurity expertise, including the development of comprehensive cybersecurity courses by institutions of higher learning, scholarships to key persons to fast-track world class cybersecurity competence, especially for persons responsible for critical infrastructure in key sectors, and for other key personnel drawn from all relevant stakeholders. Situational awareness of the cyber response teams and other users is also critical.

## People

At the centre of an effective cybersecurity initiative should be people. The measures whether policy, legislative or administrative, should be rights-respecting by design and not just pay lip service to human rights. Further, government responses to cyber threats should not be so short-sighted in that they are only directed towards enhancing government surveillance capacity to monitor and intercept communications, or criminalizing freedom of expression.

The measures should be culturally appropriate, and geared towards promoting a cyber-hygiene culture such as password policies. Further, empowering users to take responsibility for their security and to secure themselves for example through the use of multi-factor authentication. Additionally, strengthening measures to ensure the security of users for example through ensuring security by design in devices, providing users with remedies, and guaranteeing their human rights and security.

Moreover, communication to educate users should be clear, simple and consistent to ensure wider understanding of the public. Simplicity in messaging for example the Safaricom "Pin Yako, Siri Yako" campaign, and the use of common terminology in reference to cybersecurity can promote and ensure a shared understanding among the different stakeholders.  Lastly, the processes of developing cybersecurity response measures should comply with the constitutional requirement for public participation.

## ABOUT KICTANET

The Kenya ICT Action Network (KICTANet) is a non-profit organization, which acts as a multi-stakeholder platform for individuals and institutions interested and involved in ICT policy and regulation. The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development.

This publication was made possible by the generous support of Global Partners Digital and the Government of the United Kingdom.