Trust4Cyber

A study paper on human-centred cybersecurity: Kenyan Fintech sector

Authored by KICTANet and commissioned by Trust4Cyber-Flagship
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

DIGITAL TRANSFORMATION CENTER KENYA

KICTANet The Power of Communities

Imprint

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn

T +49 61 96 79-0
F +49 61 96 79-11 15
E info@giz.de
I www.giz.de/en

Programme/project description:
Global programme Digital Transformation

Project/programme title:
Trust4Cyber-Flagship

Editor/Authors:
Editorial Director: Deborah Klein, Specialist Cybersecurity, Trust4Cyber-Flagship
Authors: Grace Githaiga, Victor Kapiyo, Mwendwa Kivuva, June Okal and Ali Hussein

Design/Layout:
neues handeln AG, Berlin

Photo (Title):
Olena Yakobchuk/shutterstock.com

Location and year of publication:
Bonn 2022

Table of Contents

Executive Summary

This study maps the cybersecurity landscape in Kenya with a focus on the financial sector, and advocates for a human-centric approach in cybersecurity. It also provides the Kenyan country context in legislation, stakeholders, and the financial sector noting the increased access, use and adoption of ICTs in the country, which were facilitating the digital payments in the country, and whose value continued to grow as e-commerce became mainstream.

The study noted the progress in the development of the legal, institutional and regulatory frameworks to promote cybersecurity within the financial services sector in order to ensure secure digital transactions. Further, it maps the key stakeholders with a specific focus on actors from within the financial sector under the following overarching stakeholder groups: government, academia, civil society, technical community and the private sector.

Moreover, this study explored the cyber threat landscape giving the national cybersecurity assessment, the threats in Kenya and the region, and challenges in Kenya. It finds that there was a total of 110.9 million threats recorded in 2019/2020 with the key threats being: malware, web application attacks, botnets, distributed denial of service attacks, and system vulnerabilities. Furthermore, the study notes that the rise of digital payments has contributed to an increase in cyber threats targeting the financial sector which continues to face challenges in detection, reporting, responding and preventing cyber-attacks given the level of awareness, capacity, skills and investments to promote digital resilience among the key stakeholders.

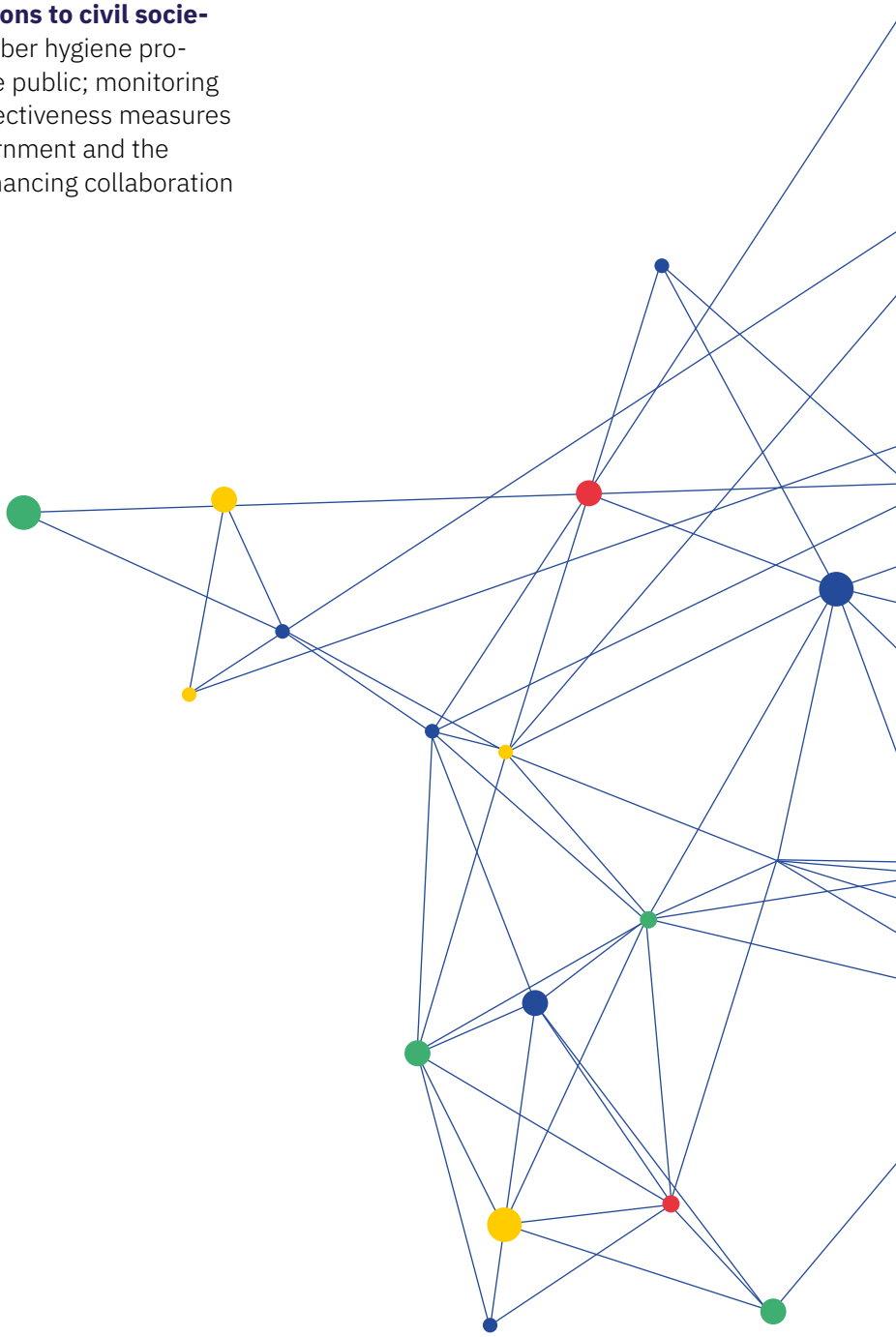
Finally, the study makes the following recommendations to the government, private sector, civil society and international development partners.

The government is called upon to among others: promote a human-centred and multistakeholder approach in the implementation of cybersecurity strategies; review the outdated cybersecurity strategy; develop a national cybersecurity policy; develop and implement a national cyber hygiene programme targeting users of financial services; enhance cybercrime information sharing, intelligence, joint cooperation between regional actors in the detection and responses to cyber incidents and the prevention of cybercrimes; and to regularly conduct national cybersecurity assessments based on international standards.

The key recommendations to the private sector include among others: investing resources towards hiring and retention of skilled personnel, knowledge and capacity building, and an upgrade of infrastructure, tools and software, as well as in cybersecurity strategies; develop cyber hygiene programmes for their users; ensure compliance with data protection laws; and to collaborate with other stakeholders in handling cyber incidents.

The key recommendations to civil society include developing cyber hygiene programmes targeted at the public; monitoring and reporting on the effectiveness measures put in place by the government and the financial sector; and enhancing collaboration with other stakeholders.

Finally, international development partners are called upon to among others: support civil society organisations to conduct research, advocacy and training; collaborate with other stakeholders; invest in capacity building programmes, information sharing, knowledge and technology transfer, and international cooperation to strengthen the synergies and capabilities between global and national actors including academia, business, government, media and civil society.



1 Introduction

The COVID-19 pandemic has highlighted the importance of digital technologies. People from all over the world are becoming more connected as a result of developments in technology, and there is an increase in digital communication tools enabled by the internet. Following the pandemic, the adoption of digital technologies has intensified across various sectors of Kenya's economy. For example, in the educational sector, the government indicated that by 2030, every school will be connected to the Internet, guaranteeing that every student has access to digital learning.[1] In addition, UNICEF has already connected 75 schools to the Internet, with a plan to connect at least 1,085 more by the end of 2021, to reach over 360,000 children. Moreover, during the pandemic, people had to rely on computer systems, mobile devices, and the Internet, for work, communication, online shopping, the exchange and receiving of information, all aimed as containment measures to the pandemic.[2]

The adoption of digital technologies has also seen an increase in cybersecurity threats and risks. This has been largely due to the rapid adoption of the digital systems, remote working without adequate attention being paid to the security of computer systems as well as increasing awareness of people on the appropriate measures to protect themselves online from cyber threats and risks. Further, cyber criminals have exploited vulnerabilities in systems leading to rising cases of cybercrimes, online child sexual exploitation, online terrorism and violent extremism, technology-based violence against women.

Kenya is one of the African countries where digitalisation is on the rise, especially in the financial sector where digital financial services are being taken up rapidly. Digitalisation in the country has enabled inclusion and access to financial services. For example, Safaricom's M-Pesa stands out as a prominent mobile money success story. Moreover, Fintechs have been able to establish creative business models using payments systems or platforms hosted by commercial banks thanks to digitization. However, even with this success, there is still the possibility that weaknesses in the systems resulting from technical breakdowns or malfunctions, human error, or cyber-attacks, could lead to widespread losses.[3] Since the start of the COVID-19 pandemic, cybersecurity risks in the financial sector have increased, with cybercriminals targeting banks, financial institutions, and fintech companies. Accordingly, the importance of cybersecurity in the Fintech sector cannot be overstated.

It is therefore increasingly important for all relevant stakeholders to be prepared to counter cyber risks and threats and ensure cybersecurity for people accessing digital financial services. More importantly, measures to promote cybersecurity should not ignore the critical role of human beings. Human rights should feature in tackling cybercrime and promoting cybersecurity. Hence, there is a need to mainstream meaningful consideration of human rights into cyber security programmes and shift the dynamic towards a human-centred security.[4]

1 UNICEF. 2021. After COVID-19, let's reimagine education in Kenya. *https://www.unicef.org/kenya/stories/after-covid-19-lets-reimagine-education-kenya*
2 Council of Europe. Cybercrime. *https://www.coe.int/en/web/cybercrime/cybercrime-and-covid-19*
3 Njuguna S. Ndungu. 2021. A Digital Financial Services Revolution in Kenya: The M-Pesa Case Study. *https://aercafrica.org/wp-content/uploads/2021/02/A-Digital-Financial-Services-Revolution-in-Kenya.pdf*
4 Making the Shift to Human-Centered Security. *https://www.forcepoint.com/sites/default/files/resources/files/transcript_making_shift_to_human_centered_security_en.pdf*

This study maps the cybersecurity landscape in Kenya with a focus on the financial sector and advocates for a human-centric approach in cybersecurity.

1.1 Understanding a human-centric cybersecurity

Cybersecurity is concerned with threats to a country's key infrastructure and is not limited to the traditional definition of national security. The concept of national security is now shaping Kenya's cybersecurity discourse, and although this strategy is sound, it is also flawed as the interventions are now focussed mostly on tech aspects and national security. However, cybersecurity should address not only a state's security concerns but also the needs of its people indicating that it is probably time for a shift to human-centric cybersecurity.

One of the most common blunders companies and firms make is treating cyber security as just an IT issue.[5] Human elements are frequently overlooked or assumed while firms focus on adopting new technologies, processes, and standards as a way of security. Yet 9 out of 10 cyber breaches in companies are a result of human error as observed in a study *Psychology of Human Error*.[6] Further, nearly half of the employees admitted they were "extremely" or "very" convinced they had made a mistake at work that had put their company's security at risk confirming the adage that the weakest link in security is in the human being. Human-centric cybersecurity can be looked at from a data perspective, and where human factors are the major engine and enabler of cyber techniques.

From the data perspective, Richard Ford[7] argues that the "traditional, tech-centric approach" gives a lot of control to online attackers. He considers human-centred security, as that point of contact between the human and the data and assuring that the data is most available and most valuable to a person. Meaning that data requires protection even when most at risk. Where cyber-attacks are concerned, data is most valuable to an individual when at a point of access, and when being utilised by another person. This is also where data is most vulnerable. At this point, a human-centred cybersecurity is looked at as the point of interaction between the human and the data. Where access to data is concerned, this could be through a malicious insider, an accidental insider, or a compromised insider. When ransomware happens, and a person's data is gone, there is the realisation that what was valued on a computer was the data. There is, therefore, a need to firstly focus on the human perspective and access to data, before understanding what data is.[8] In addition, a human-centric approach is not just about giving a user the information they need to make the best decision; but it is about giving them the information in a way that encourages the right behaviour when it comes to how they handle data and manage cybersecurity breaches.

Conventional cybersecurity is tech-oriented and not about people. It is anchored on attacks, threats, and the vulnerability of systems, yet human factors play a role. Usually, there is concern about a brand-new exploit or a new piece of malware, meaning that attention is focused on the attacker. Companies cannot expect employees to practice good cyber hygiene if they are often excluded from cyber operations due to complicated technical phrases. This is what must be altered. For companies, the truth is that cybersecurity is not solely the realm of security

5 460 degrees. Human Centric Cybersecurity. *https://www.460degrees.com/expert-capabilities/human-centric-cyber-security/*

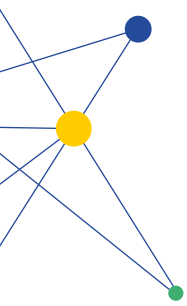
6 CISOMAG. 2020. Psychology of Human Error" Could Help Businesses Prevent Security Breaches. *https://cisomag.eccouncil.org/psychology-of-human-error-could-help-businesses-prevent-security-breaches/#:~:text=A%20joint%20study%20from%20Stanford,if%20organizations%20judge%20them%20severely.*

7 Information, Security Media Group. Making the Shift to Human-Centered Security. *https://www.forcepoint.com/sites/default/files/resources/files/transcript_making_shift_to_human_centered_security_en.pdf*

8 Information, Security Media Group. Making the Shift to Human-Centered Security. *https://www.forcepoint.com/sites/default/files/resources/files/transcript_making_shift_to_human_centered_security_en.pdf*

experts.[9] Every single employee within a firm has a hand in the organisation's security as they handle, manipulate, and communicate company data as part of their duties. It is therefore critical to provide people the tools they need to comprehend anomalous behaviour, detect it, respond to it, and report across the organisation. To strengthen cybersecurity and empower employees, companies must embrace an approach that places the human as central.

What is important to note is that human-centric cybersecurity works in tandem with cybersecurity defence technology to achieve optimal efficacy.



Cybersecurity in Kenya is looked at, as the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorised access, change or destruction.[10] This is a tech-based definition which has not entirely embraced the practice of implementing public communication as a tool to educate the public on what measures they should take to engage in a secure online space. Many ordinary citizens lack the knowledge and awareness of cyber-attacks and yet their predominant transactions nowadays are through mobile money. This is an indication that there is a need to increase capacity on risks and skills/knowledge on cybersecurity in the public sector particularly targeting financial services/products and their usage.[11]

Accordingly, there is a need to consider the human element in different interventions when it comes to awareness and operationalization of cybersecurity policy, which will allow for a more robust understanding of ICT laws and regulations.[12] In addition, the relevant authorities such as CIRTs and National Cyber Command and Coordination Centre (NC4) need to hold regular consultative fora to share information on policies and discuss implementation with citizens with emphasis on the role of humans in cybersecurity.

1.2 Country Context

An increase in data and internet subscriptions in Kenya has been observed especially after the lockdown that was put in place by the government of Kenya during the COVID-19 pandemic. According to the Communications Authority, 64.4 million active mobile subscriptions (SIM cards) were recorded as of 30th June 2021.[13] This was a 2.4 million net addition in mobile subscriptions from the previous quarter (January to March 2021). The overall number of SMS transmitted from local mobile networks rose by 20.8 percent from the previous quarter to stand at 12.8 billion.[14] The overall number of international incoming and outgoing mobile voice minutes increased by 4.3 percent and 8.6 percent, respectively, to 116.9 million and 135.9 million minutes. During the same period, the number of international incoming mobile SMS climbed by 30.3 percent to 10.9 million, while the amount of international outgoing mobile messages decreased by 10.9 percent to 8.3 million.[15]

There has also been an uptake of broadband services and ICT services. For example, the overall number of active Internet/data subscribers stood at 46.7 million in the third quarter of 2021, up from 43.7 million in the third quarter of the previous year.

9 Ran Pugach. Demystifying cybersecurity with a more human-centric approach. 2021. *https://www.helpnetsecurity.com/2021/08/06/cybersecurity-human-centric-approach/*
10 Githaiga, G and Victor Kapiyo. 2019. Kenya's Cybersecurity Framework: Time to Up the Game! *https://www.kictanet.or.ke/?mdocs-file=41288*
11 Stiftung Neue Verantwortung. Cybersecurity Policy Exercise Kenya.
12 Stiftung Neue Verantwortung. Reflections at the Cybersecurity Policy Exercise Kenya. 5th of October 2021
13 Communications Authority. Sector Statistics Report Q4 2020-2021. *https://www.ca.go.ke/document/sector-statistics-report-q4-2020-2021/*
14 Communications Authority. Sector Statistics Report Q4 2020-2021. *https://www.ca.go.ke/document/sector-statistics-report-q4-2020-2021/*
15 Communications Authority. Sector Statistics Report Q4 2020-2021. *https://www.ca.go.ke/document/sector-statistics-report-q4-2020-2021/*

When compared to the 40.9 million subscriptions reported during the same period of the 2019/2020 Financial Year, this is a 12.8 percent increase. Broadband subscriptions stood at 27.5 million and accounted for 97.4 percent of the total broadband subscriptions. Notably, mobile data subscriptions still account for more than 99 percent of all data subscriptions. This increased uptake of mobile and data subscriptions, and a rise in online communication, have meant that people, some of whom may be engaging with these technologies for the first time, are exposed to more cybersecurity risks.

1.3 Why the financial sector

The private sector continues to be a major engine of economic growth. The sectors driving this growth and key to the overall economy and stability of the financial sector include Manufacturing, Trade, Households, and Real Estate.[16] The insurance, capital markets, banking, insurance, pensions, and Sacco societies industries, and unregulated financial services companies, make up Kenya's financial system. This financial system is backed up by a strong financial markets infrastructure that makes payments, settlements, and custodial services easier.[17] FinTech adoption has also resulted in a transformation of the sector in terms of products and services and for example, there are 23.8 million MPesa users.[18] During the 2020/21 fiscal year, Safaricom extended $3.1 billion in Fuliza credit. Fuliza gives an estimated $12 million credit to Kenyans every day.[19] A total of KSh 242 billion was calculated using the KPMG True Value Bridge, an indication that M-PESA has created a lot of social value.[20] There has also been a proliferation of digital lenders with more than 100 operating in Kenya[21] with such examples as Tala, Okash and Opesa.

Kenya's government has adopted digital finance and online self-service platforms as a means of delivering services. Digital platforms such as the Kenya Revenue Authority's (KRA) iTax platform, the eCitizen portal, the National Transport and Safety Authority's (NTSA), Transport Integrated Management System (TIMS), the Integrated Financial Management System (IFMIS), the Integrated Election Management System (KIEMS), the Integrated Population Registration Services (IPRS), National Integrated Identity Management System (NIIMS) also referred to as Huduma Namba[22] recently declared unconstitutional,[23] are just a few of the key e-government platforms.

That notwithstanding, the volume of RTGS stood at 0.5 million valued at KES 3.2 trillion (USD 28.3 billion)[24] in September 2021, while there were 1.2 million Electronic Fund Transfer (EFT) transactions valued at KES 66.40 billion (USD 589 million).[25] In addition, 1.4 million cheques were issued valued at KES 216.98 billion (USD 1.924 billion).

16 Central Bank. Kenya Financial Stability Report. *https://www.centralbank.go.ke/uploads/financial_sector_stability/1560356005_Financial%20Stability%20Report.pdf*
17 ibid.
18 Techcrunch. Mobile overdraft facility Fuliza outshines Silicon Valley-backed lending apps in Kenya. 2021. *https://techcrunch.com/2021/12/17/mobile-overdraft-facility-fuliza-outshines-silicon-valley-backed-lending-apps-in-kenya/*
19 Ibid.
20 Safaricom. Standing together: Going beyond. 2021. *https://www.safaricom.co.ke/images/Downloads/Safaricom_2021_Sustainable_Business_Report.pdf*
21 Annie Njanja. 2021. Kenya cracks down on digital lenders over data privacy issues. *https://techcrunch.com/2021/10/25/kenya-cracks-down-on-digital-lenders-over-data-privacy-issues/*
22 Githaiga, G and Victor Kapiyo. 2019. Kenya's Cybersecurity Framework: Time to Up the Game! *https://www.kictanet.or.ke/?mdocs-file=41288*
23 Justice Initiative. 2021. New Kenya High Court Judgement Sets Important Precedent for Digital ID Privacy Protections and Processes. *https://www.justiceinitiative.org/newsroom/new-kenya-high-court-judgment-sets-important-precedent-for-digital-id-privacy-protections-and-processes*
24 Central Bank of Kenya. KEPSS/RTGS. *https://www.centralbank.go.ke/national-payments-system/kepss-rtgs/*
25 Central Bank of Kenya. Cheques & EFTs. *https://www.centralbank.go.ke/national-payments-system/automated-clearing-house/cheques-efts/*

Digital financial services (DFS) have a lot of promise to enhance people's lives by enabling financial inclusion. Yet cybercrime has emerged as a major worry in the financial world and threatens to hinder progress toward financial resilience.

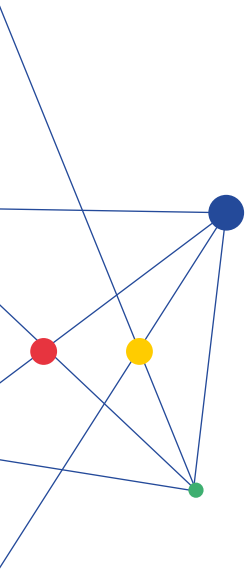
The National Payment System (NPS) Act of 2011 was passed in Kenya, creating a new legal foundation for NPS. This legislation established rules for the regulation and oversight of payment systems and payment service providers, as well as other related matters.[26] In addition, the National Payment System Regulations 2014 was enacted to put into effect the NPS Act 2011. It provides for the authorisation and control of payment service providers, the designation of payment systems, the designation of payment instruments, and Anti-Money Laundering procedures. The Central Bank of Kenya in 2017 gave a Guidance Note on Cybersecurity that defines cybersecurity, cyberism and critical information infrastructure among other key terms.[27] It identifies the minimum requirements that institutions should have to mitigate cyber risk and in Article 2.1 states the purpose of note as:

- Create a safer and more secure cyberspace that underpins information system security priorities and promote stability of the Kenyan banking sector;
- Establish a coordinated approach to the prevention and combating of cybercrime;
- Up-scaling of identification and protection of critical information infrastructure;
- Promotion of compliance with appropriate technical and operational cybersecurity standards;
- Development of requisite skills, continuous building of capacity and promote a culture of fostering a strong interplay between policy, leveraging on technology to do business and risk management; and
- Maintenance of public trust and confidence in the financial system.
- The Guidance note is a response to the challenges in the cyberspace environment. However, it needs to be reviewed regularly in line with the dynamism of this cyberspace and the emerging challenges.

Accordingly, any modern payment system must have security as a feature in terms of how the system functions with strong safeguards, as well as how it mitigates existing and future cyber-risk threats. The top two significant worries from the financial sector and stakeholders are cyber threats and fraud.[28] Hence, Kenya will attract more users to its NPS if it strengthens its defences against existing and future threats, promoting uptake and lowering system and product dormancy.

Mobile money services have become more popular as a result of more businesses such as banks, and organisations digitising their processes. In September 2021, the total active mobile money agents were 305,831, with an overall 67.7 million registered mobile money accounts.[29] The volume of agent cash out transactions stood at 180.85 million valued at KES 585.38 billion (USD 5.19 billion). The total number of active registered telecom mobile money subscriptions stood at 34.7 million during quarter 4 of 2021.[30] The last year has seen a rise in mobile money transfer services, which can be attributed to increased consumer adoption of digital payments in an effort to curb the spread of COVID-19. For example, in 2020, revenue from mobile services was KES 280.1 billion (USD 2.48 billion), up 1.3 percent over 2019. In addition, mobile sub-sector investments rose by 28.9 percent to KES 45.9 billion (USD 407.17 million) in 2019, up from KES 35.6 billion in 2018.[31]

26 Central Bank of Kenya. National Payments System. *https://www.centralbank.go.ke/national-payments-system/*
27 Central Bank of Kenya. Guidance Note on Cybersecurity for the Kenyan banking sector in August 2017. *https://www.centralbank.go.ke/wp-content/uploads/2017/09/GUIDANCE-NOTE-ON-CYBERSECURITY-FOR-THE-BANKING-SECTOR.pdf*
28 Central Bank of Kenya. Kenya's National Payments System and Strategy 2021 – 2025. *https://www.centralbank.go.ke/wp-content/uploads/2020/12/CBK-NPS-Vision-and-Strategy.pdf*
29 Central Bank of Kenya. Mobile payments. *https://www.centralbank.go.ke/national-payments-system/mobile-payments/*
30 Communications Authority. Sector Statistics Report Q4 2020 – 2021. *https://www.ca.go.ke/wp-content/uploads/2021/09/Sector-Statistics-Report-Q4-2020-2021.pdf*
31 Ibid.



The 2021 annual Financial report produced by the Central Bank of Kenya[32] notes that at the onset of COVID-19, the Information and Communications sector became "the rail guards for financial transactions, information dissemination, and virtual workstreams. The banking sector for example adopted technology to enhance the banking sector and its services with a focus on digitization of businesses; banking and fintech; data governance; and future developments in the ICT sector among others.[33] However, the report highlights that cybersecurity is one of the risks in the financial sector and goes to cite the example of the insurance industry which has seen an increased measure of cyberattacks. This is attributed to the lack of security in home-based setups when working remotely. Furthermore, the number of frauds has increased as fraudsters attempt to defraud naïve policyholders or even insurers.

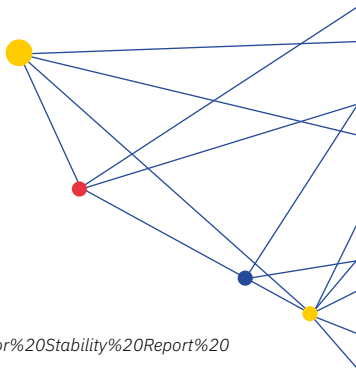
Attacks on the financial sector and banking services happen using malicious software to disseminate spam emails containing malicious links and attachments. These were used to infect users' computers and insert keyloggers onto them, allowing threat actors to steal banking credentials.[34] Accordingly, as cyber threats continue to be a threat and undermine financial resilience, areas targeted for fraud and which the financial sector must be alert to include ATM infrastructure, mobile banking infrastructure, third parties and vendors, and debit and credit systems. Another area at risk of sabotage and ransomware in the financial sector are identity management systems.[35]

With the Kenya citizens adopting online e-commerce and mobile transactions to procure goods and services, e-skimming and credit card fraud have increased where cyber threat actors infiltrate e-commerce websites with malicious code in order to intercept buyers' credit card credentials when they make purchases on the affected sites.[36] Here, the cyber threat actors steal critical data such as user information that includes credit card details, usernames and passwords. This information is either sold or utilised to make fraudulent purchases.

It is important for stakeholders to design policy, legal and regulatory interventions to tackle cybercrime. By drastically decreasing the chances of a breach, organisations can be better protected from the enormous financial and productivity losses, as well as downtime, that a cyber-attack can cause.

1.4 Methodology

The methodology adopted for the study included a literature review of publications on cybersecurity threats including in the financial sector; policy and regulatory reports, print and digital media reports, and government documents. In addition, Stakeholders' reflections at the Cybersecurity Policy Exercise Kenya, and Workshop outcomes of a Cybersecurity Policy Exercise in Kenya undertaken by Stiftung Neue Verantwortung (SNV) for GIZ in October 2021; and comments gathered during a Trust4Cyber-Flagship at GIZ and KICTANet Webinar on Financial products and Services – How to make users cyber-resilient. Dos and Don'ts, held on 9th December 2021 during Kenya's innovation week were reviewed and are part of this study.



32 Central Bank of Kenya. Kenya Financial Sector Stability Report 2021. *https://www.centralbank.go.ke/uploads/financial_sector_stability/48936558_Kenya%20Financial%20Sector%20Stability%20Report%202020.pdf*

33 Central Bank of Kenya. Bank Supervision annual report 2020. *https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/468154612_2020%20Annual%20Report.pdf*

34 National Ke-CIRT/CC. Cybersecurity Report. April to June 2021. *https://ke-cirt.go.ke/wp-content/uploads/2021/08/Quarter-4-FY-2020_21-National-KE-CIRT_CC-Cybersecurity-Report-Public-Version.pdf*

35 Serianu Ltd. Africa Cybersecurity Report: Kenya 2019/2020. *https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf*

36 National Ke-CIRT/CC. Cybersecurity Report. April to June 2021. *https://ke-cirt.go.ke/wp-content/uploads/2021/08/Quarter-4-FY-2020_21-National-KE-CIRT_CC-Cybersecurity-Report-Public-Version.pdf*

2 Cybersecurity Policy and Legal Framework

This section provides a brief highlight of the cybersecurity policy and legal frameworks for Kenya.

2.1 National Laws and Policies

Kenya has developed several policies, laws, strategies and guidelines that are relevant for cybersecurity. They include among others: the National Information, Communications and Technology (ICT) Policy, the National Cybersecurity Strategy 2014, the National ICT Master Plan 2014 – 2018, Digital Economy Blueprint, Guidance Note on Cybersecurity for the Banking Sector, Central Bank of Kenya Act, The Kenya Information and Communication Act, Computer Misuse and Cyber Crimes Act, 2018, and the Data Protection Act, 2019.

National Information, Communications and Technology (ICT) Policy[37] – The mission of the policy is to "facilitate universal access to ICT infrastructure and services all over the country." The policy covers four key objectives including: mobile first; market; skills and Innovation; and public service delivery. The policy identifies cybercrime and cybersecurity vulnerabilities as emerging issues for attention. The key cyber security priorities under the policies include among others: recognising cybersecurity as a key pillar of national security; foster a multi-agency approaches; establish an enabling legal framework; support the development of technologies that will lead to measurable, available, secure, trustworthy, and sustainable computing and communications systems; develop information security standards for the ICT sector; sensitise and create awareness; ensure the efficient mitigation of cyber threats in order to promote trust and confidence; and put in place measures to protect vulnerable groups; and develop intelligence, defensive and offensive capabilities.

In order to implement the policy, the government has committed to among others: implement Computer and Cyber Crimes Legislation; promote confidence and trust in the use of ICTs; enacting specific and effective legislative instruments on privacy, security, cybercrimes, ethical and moral conduct, encryption, digital signatures, copyrights and fair trade practises; addressing gaps in regulatory capacity; leverage on the power of ICTs to assist law enforcement agencies and defensive agencies to secure borders; require ICT Service Providers to provide facilities for emergency communication and prediction, monitoring and early warning of disasters; and identify critical infrastructure.

The adoption of the policy took almost three years since 2016, when the first draft was completed, leading to a lull during its development process.[38] Efforts are already underway to develop legislation on the protection

37 National Information, Communications and Technology (ICT) Policy, *https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf*

38 KICTANet, Public participation: An Assessment of Recent ICT Policy Making Processes in Kenya, *https://www.kictanet.or.ke/?mdocs-file=43918*

of critical infrastructure, and a bill is expected to be published by the National Assembly. At the same time, the implementation of the contentious Computer Misuse and Cybercrimes Act, 2018 continues after several legal challenges to the constitutionality of the law.

The National Cybersecurity Strategy 2014[39] – This strategy outlines the country's cybersecurity goals which includes the following: To enhance the nation's cybersecurity posture; build national capability; foster information sharing and collaboration and provide national leadership. Further, it proposed a number of measures including creating an overarching governmental 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. Moreover, it proposes additional measures such as 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.

While this strategy made critical proposals to strengthen Kenya's cybersecurity posture, only a few of the measures proposed under the strategy were achieved. Key among this was the bestowing of cybersecurity responsibility to the Communications Authority, where the national CIRT is based. Nonetheless, key gaps that remain undefined include the lack of a clear cybersecurity policy and an effective coordination framework. Currently, efforts are underway to review the strategy which is long overdue. However, what will be important is the monitoring and implementation of the strategies that will be developed.

The National ICT Master Plan 2014 – 2018[40] – The vision of the Masterplan is to establish "Kenya as a regional ICT hub and a globally competitive digital economy" with its guiding principles being partnership; equity and non-discrimination; technology neutrality; environmental protection and conservation; good governance; and incentivizing. It provides a roadmap to transition the country into a knowledge society and aims to position the country as a regional ICT Hub by developing quality ICT infrastructure, integrated and secure information infrastructure and a critical mass of high-end ICT human capital.

Further, 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 institutionalisation of a middleware platform to enable secure data and information access; and the development of a cybersecurity policy. This is behind the vision of increasing and strategically implementing "one-stop, non-stop e-government services" across the entire public sector. Part of the successful proposals of the masterplan include the adoption of data protection legislation and the Office of the Data Protection Commissioner, and the development of the eCitizen platform. However, the cybersecurity policy that was proposed was not developed in the end.

39 National Cybersecurity Strategy 2014, Ministry of ICT, Republic of Kenya, *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf*

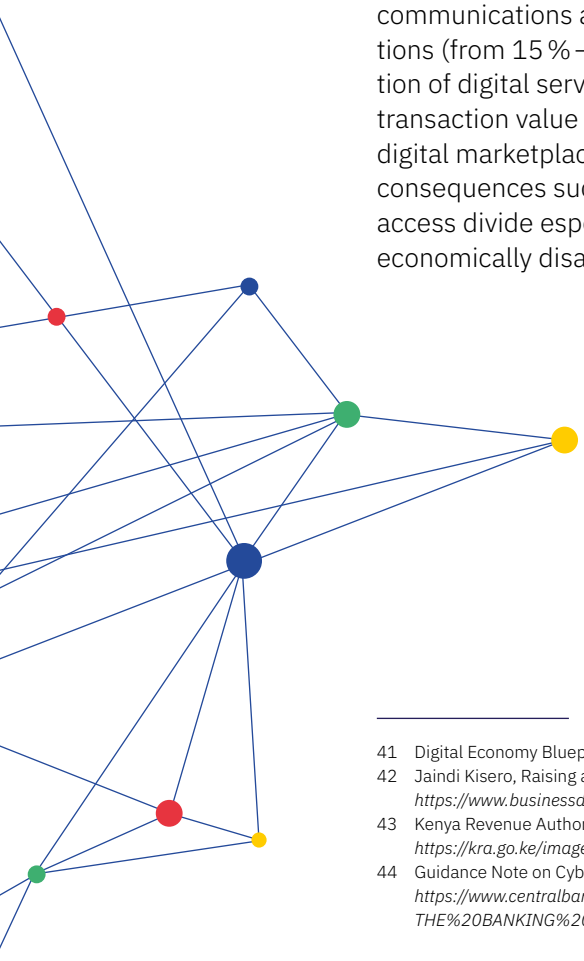
40 National ICT Master Plan 2014 – 2017, Ministry of ICT, Republic of Kenya, *https://academia-ke.org/library/download/mict-kenya-national-ict-masterplan-2014-2017/?wpdmdl=7207&refresh=61ffb62adebf51644148266*

Digital Economy Blueprint[41] – The Blueprint which provides the framework for a successful and sustainable digital economy, recognises the central role of cybersecurity as an enabler for the "protection of the integrity of electronic and digital systems is a paramount concern in a digitally enabled economy." Moreover, that cybersecurity is essential for the development of the digital economy. The blueprint prioritises data security, privacy, and child online safety as part of the strategy to foster confidence and trust and security of the digital economy. Further, it identifies the reforms in laws, regulations and institutional frameworks to ensure data security.

The policy which was developed largely without broad stakeholder participation makes broad commitments on various aspects of the ICT sector and the digital economy. However, the recent developments within the ICT seem to suggest little synchronisation of government actions with the blueprint or a coherent approach towards promoting a digital economy. For example, recent and indiscriminate excise tax increases on internet data communications and mobile money transactions (from 15 % – 20 %),[42] and the introduction of digital service taxes (1.5 % of gross transaction value of services or fees paid in a digital marketplace)[43] could have unintended consequences such as increasing the digital access divide especially for marginalised and economically disadvantaged users.

Guidance Note on Cybersecurity for the Banking Sector[44] – The Note outlines the minimum requirements to ensure effective cybersecurity governance and risk management frameworks for banking institutions. Further, it calls for institutional reforms in banking institutions including the creation of cyber risk roles for the Board of Directors, Senior Management, and Chief Information Security Officers. Moreover, it provides practical guidance to the institutions including 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. Also, it further highlighted the risks that could emanate from outsourcing, cloud providers and other services to save time and reduce operation costs. Lastly, it requires banking institutions to review and submit their revised Cybersecurity Policy, strategies and frameworks to CBK by November 30, 2017.

This note was developed at the backdrop of increased cyber-attacks and losses within the financial sector, as many of the institutions were reported (as discussed above) to have suffered massive losses through cybercrimes and poor cyber security practises. The Note provides a good basis for these institutions to take measures to safeguard their cybersecurity. It will therefore be important to monitor its implementation amidst rising use of mobile money transactions, online banking and e-commerce transactions.



41 Digital Economy Blueprint, Ministry of ICT, *http://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf*
42 Jaindi Kisero, Raising airtime, data taxes is a bad call, Business Daily Africa, *https://www.businessdailyafrica.com/bd/opinion-analysis/columnists/raising-airtime-data-taxes-is-a-bad-call-3458022*
43 Kenya Revenue Authority, Introducing Digital Service Tax, *https://kra.go.ke/images/publications/Brochure-Digital-Service-Tax-Website.pdf*
44 Guidance Note on Cybersecurity for the Banking Sector, Central Bank of Kenya, August 2017, *https://www.centralbank.go.ke/uploads/banking_circulars/634077191_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf*

Cybersecurity Guideline for Payment Service Providers (PSPs)[45] – The objective is to create a safer and more secure cyberspace that underpins information system security priorities, to promote stability of the Kenyan payment system sub-sector. The Guideline sets the minimum standards that PSPs are required to adopt in order to develop and implement effective cybersecurity governance and risk management frameworks. It further outlines the minimum requirements that PSPs are required to build upon in the development and implementation of strategies, policies, procedures and related activities for mitigating cyber risk.

Draft Central Bank of Kenya (Digital Credit Providers) Regulations, 2021[46] – These draft regulations were published in December 2021 to provide a framework for the licensing and regulation of digital credit providers. It also regulates in Part IV, the conditions under which digital credit providers may share or exchange credit information with credit reference bureaus; requires the provision of a customer's consent prior to the submission or sharing of credit information; and restricts the sharing with third parties or use of credit information obtained from bureaus other than for the intended purpose. Moreover, the regulations in Part VII provides for consumer protection, including requiring providers to: establish complaints redress mechanisms; use systems that are secure to ensure information confidentiality and security; provide comprehensive terms and conditions; ensure advertising is not false among others. Moreover, under clause 24, digital credit providers are obliged to educate consumers not only on the services, but also to enable them to be aware of the need to "keep their personal details and information such as Personal Identification Number (PIN) secure". Lastly, the providers are required under clause 15(3) to take measures to safeguard the security of the information provided to them or issued by them to credit reference bureaus.

The Central Bank of Kenya Act[47] – This law establishes the Central Bank of Kenya including its roles, functions and management. It also provides for the regulation of aspects such as the national currency, external relations, the regulation of foreign exchange dealings, and relations with public entities. The key objectives of the bank are to: formulate and implement monetary policy directed to achieving and maintaining stability in the general level of prices; foster the liquidity, solvency and proper functioning of a stable market-based financial system; and to support the economic policy of the Government, including its objectives for growth and employment. In 2021, amendments were proposed to the Act under the Central Bank of Kenya (Amendment) Bill, 2021[48] granting the Bank power under section 4A(1)(da) to "license and supervise digital credit providers not regulated under any other written law," who the Act requires to register with the Bank within six months of coming into force of the Act. The Bank was also empowered under section 33R to regulate digital lenders. Moreover, an amendment to section 57(2) empowers the Bank to make regulations necessary to cover aspects such as: credit information sharing, data protection and consumer protection.

Prior to the amendments, there had been concerns including from the Central Bank regarding the lack of an appropriate regulatory framework for digital lenders leading to unpredictability in the market. Whereas lenders had invested in the country's credit market in response to the appetite for quick loans, it had created new challenges. There are at least 100 digital applications operating

45 Cybersecurity Guideline for Payment Service Providers (PSPs), *https://www.centralbank.go.ke/2019/07/05/cybersecurity-guideline-for-payment-service-providers/*

46 Draft Central Bank of Kenya (Digital Credit Providers) Regulations, 2021, *https://www.centralbank.go.ke/uploads/banking_circulars/673866074_DRAFT%20DIGITAL%20CREDIT%20PROVIDERS%20REGULATIONS%202021%20-%20December%202021.pdf*

47 Central Bank of Kenya Act, *https://centralbank.go.ke/images/docs/The_Central_Bank_of_Kenya_Act_1st_January_2014.pdf*

48 Central Bank of Kenya (Amendment) Bill, 2021, *http://www.parliament.go.ke/sites/default/files/2021-05/Central%20Bank%20of%20Kenya%20%28Amendment%29%20Bill%2C%202021.pdf*

in the country,[49] offering an estimated KES 4 billion loans monthly,[50] whose operators had been accused of charging exorbitant interest rates of up to 520 percent when annualised, using exploitative terms and conditions in contracts, using threats and debt-shaming tactics to recover debts, and abusing confidentiality of customers by unlawfully sharing personal data of borrowers and defaulters with data analytics firms and for marketing.[51] Eyes will now be on the Bank as it reigns in on digital lenders.

The Kenya Information and Communication Act[52] – The Act defines cybersecurity as the "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practises, assurance and technologies that can be used to protect the cyber environment". The Act requires the Cabinet Secretary, in consultation with the Authority, to make regulations with respect to cybersecurity and at the same time, provides for a Public Key Infrastructure (PKI) framework as a means of securing online transactions.

Moreover, it provides for the functions of the Commission in relation to electronic transactions and cyber security under section 83C which include among others to: facilitate electronic transactions by ensuring the use of reliable electronic records; facilitate electronic commerce and eliminate barriers to electronic commerce; promote public confidence in the integrity and reliability of electronic records and electronic transactions; foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium; promote and facilitate efficient delivery of public sector services by means of reliable electronic records; develop sound frameworks to minimise the incidence of forged electronic records and fraud in electronic commerce and other electronic transactions; promote and facilitate the efficient management of critical internet resources; and develop a framework for facilitating the investigation and prosecution of cybercrime offences.

Computer Misuse and Cyber Crimes Act, 2018[53] – The objectives of the law include among others to: protect the confidentiality, integrity and availability of computer systems, programs and data; prevent the unlawful use of computer systems; facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes; protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and facilitate international co-operation on matters covered under the Act.

The law establishes the National Computer and Cybercrimes Co-ordination Committee whose mandate include among others: co-ordinating national security organs; receiving and acting on reports; developing framework for critical national information infrastructure; co-ordinating collection and analysis of cyber threats, and response to cyber incidents; co-operating with computer incident response teams and other relevant bodies; establishing codes of cybersecurity practice and standards of performance for owners of critical national information infrastructure; developing and managing the national public key infrastructure framework; and developing frameworks for training on prevention, detection and mitigation of computer and cybercrimes.

49 Kenya cracks down on digital lenders over data privacy issues, *https://techcrunch.com/2021/10/25/kenya-cracks-down-on-digital-lenders-over-data-privacy-issues/*

50 Digital lending in Kenya: an urgent case for regulation, *https://www.dlapiperafrica.com/en/kenya/insights/2021/digital-lending-in-kenya-an-urgent-case-for-regulation.html*

51 Digital lenders under probe for sharing defaulters data, *https://www.businessdailyafrica.com/bd/economy/digital-lenders-under-probe-sharing-defaulters-data-3613676*

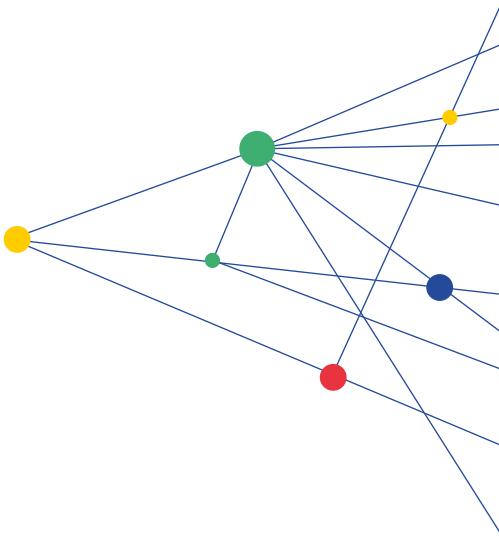
52 The Kenya Information And Communications Act Chapter. 411A, *http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%201998*

53 Computer Misuse and Cyber Crimes Act, 2018, *http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018*

The implementation of the law was plagued with legal challenges from its enactment. In April 2018, a lawsuit was filed resulting in the suspension of 27 provisions of the Act.[54] In February 2020, the High Court found the law to be constitutional, a decision which has yet again been appealed at the Court of Appeal, which is yet to render its decision.[55] In another case in June 2020 relating to the same law, the High Court found the Act to have been unconstitutionally passed, but the decision was reversed in 2021.[56] In 2021, a contentious amendment to the law was proposed that sought to ban pornography and expand the powers of the National Computer and Cybercrimes Committee to recommend websites that would be inaccessible within the republic.[57] These amendments are still under consideration before Parliament. In October, the government constituted the National Computer and Cybercrimes Committee (NC4), and it is yet to be seen how the government-only committee shall galvanise and coordinate non-government stakeholders to promote cybersecurity within the country.

The Data Protection Act, 2019[58] – The objectives of the Act are, among others, to: regulate the processing of personal data; ensure that the processing of personal data of a data subject is guided by the data protection principles; protect the privacy of individuals; establishes the Office of the Data Protection Commissioner to protect personal data; and to provides data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act. The data protection principles include the requirement for data controllers and processors to process data lawfully; minimise collection of data; restrict further processing of data; ensure data quality; restrict transfer of personal data and to establish and maintain security safeguards to protect personal data. The Act also provides the framework for the registration of data controllers and processors and provides penalties for their breach of their obligations under the Act.

So far, the Data Protection Commission has been established, though it currently remains largely understaffed and lacks the capacity to effectively discharge its mandate. Despite these shortcomings, the Commission has published its Strategic Plan, Service Charter, a Guidance Note on Data Protection Impact Assessments, Guidance Note on Consent, a Complaints Management Manual and draft regulations such as the: Data Protection (General) Regulations, 2021, Data Protection (Compliance and Enforcement) Regulations, 2021 and the Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021. These regulations are yet to come into force but shall be expected to play a key role in how personal data will be protected and enforced in the coming years.



54 BAKE To Challenge The Constitutionality Of The Computer Misuse And Cybercrimes Act, *https://www.blog.bake.co.ke/2018/05/17/bake-to-challenge-the-constitutionality-of-the-computer-misuse-and-cybercrimes-act/*

55 High Court Declares the Computer Misuse and Cybercrimes Law "Constitutional", *https://techweez.com/2020/02/20/court-declares-computer-and-cybercrimes-law-constitutional/*

56 Win for Senate in supremacy war as court declares 23 laws unconstitutional, *https://www.standardmedia.co.ke/nairobi/article/2001391976/judges-strike-out-23-laws-that-mps-passed-illegally*

57 Kenya: Withdraw proposed amendments to cybercrimes law, *https://www.article19.org/resources/kenya-withdraw-proposed-amendments-to-cybercrimes-law/*

58 The Data Protection Act, 2019, *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf*

2.2 Regional Instruments

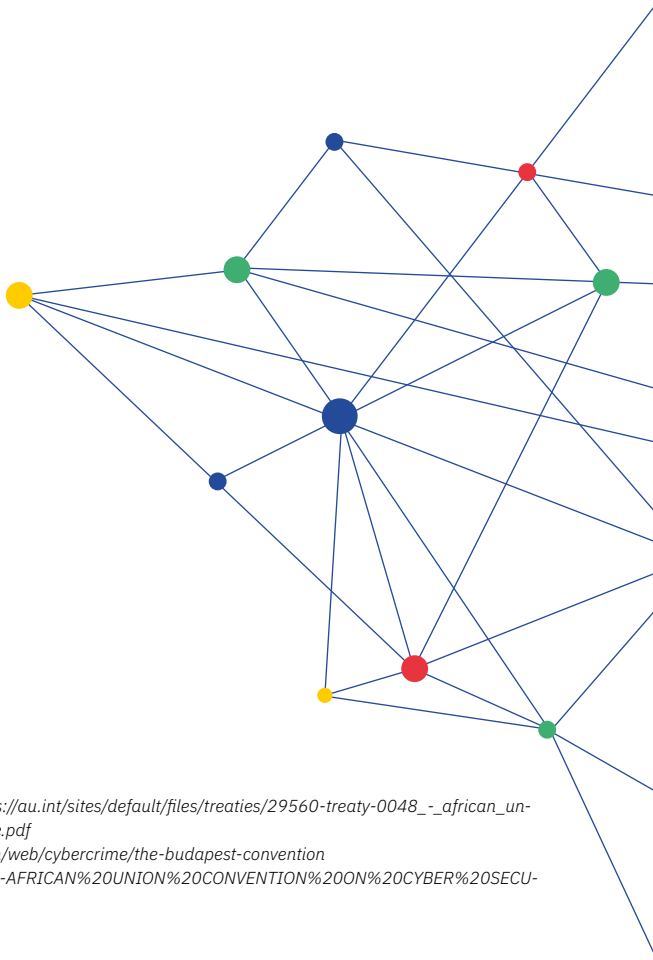
At the regional level, Kenya is not a signatory to the African Union Convention on Cyber Security and Personal Data (Malabo Convention)[59] or the Council of Europe's Convention on Cybercrime.[60] The Malabo Convention seeks to set essential rules to address the gaps in regulation of electronic communications and signatures; and the absence of rules to protect consumers, intellectual property rights, personal data and information and information systems and privacy online. More specifically, to establish minimum standards and procedures on security issues and provide harmonised legislation to enhance cooperation on cybersecurity by Member States.

The Convention calls upon Member States to put in place measures, including among others: formulating national cybersecurity policies and strategies; adopting legislative measures to address cybercrimes; establishing and conferring responsibility to respond to cybersecurity; protecting critical infrastructure; and respecting the rights of citizens. Moreover, states are encouraged to promote a culture of cybersecurity among all stakeholders, including by implementing programmes to sensitise network users, encouraging development of cybersecurity culture in enterprises, and launching elaborate sensitization campaigns for internet users, small businesses, schools and children.

The Convention calls upon Member States to put in place measures, including among others: formulating national cybersecurity policies and strategies.

In addition, it seeks to develop and foster public-private partnerships to engage industry, civil society and academics to promote and enhance the culture of cybersecurity. Since its adoption in June 2014, it has so far been signed by 14 countries and ratified by eight countries.[61] It is not apparent why states are reluctant to fast-track its adoption, which hinders the uniformity of practice in cybersecurity across various African countries. Nonetheless, Kenya's national CERT is a member of the AfricaCert which is a continental forum of continental response teams which among others, assists in the coordination of cooperation among Computer Security Incident Response Teams (CSIRTs) in the region.[62]

It is not apparent why the government is reluctant and has not taken steps to ratify these instruments despite being one of the states priding itself to be an ICT leader in the region. However, it is worth noting that legislations such as the Computer Misuse and Cybercrimes Act, 2018 and the Data Protection Act, 2019 have embedded proposals contained in the twin instruments.



59 African Union Convention on Cyber Security and Personal Data, *https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf*

60 Council of Europe, Convention on Cybercrime, *https://www.coe.int/en/web/cybercrime/the-budapest-convention*

61 Ratification status, *https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf*

62 AfricaCert, About Us, *https://www.africacert.org/about-us/*

3 Stakeholders

This section maps all relevant stakeholders in the field of cybersecurity in Kenya with a specific focus on actors from within the financial sector under the following overarching stakeholder groups: government, academia, civil society, technical community and the private sector.

3.1 Government

Ministry of Interior & Coordination of National Government – The State Department for Interior is mandated to keep the country safe and secure with key responsibilities apportioned to two of the country's national security organs, i. e., the National Intelligence Service (NIS) and the National Police Service (NPS), both of which work in tandem with the National Security Council. The Department is also responsible for coordinating all National Government functions and development projects and programmes in counties.

Directorate Criminal Investigation – The Directorate of Criminal Investigations collects and provides criminal intelligence and undertakes investigations on serious crimes including money laundering and economic crimes. Among other crimes, the Directorate investigates Cyber Crime and Financial & Hi-tech Crimes and hosts the Digital Forensic Laboratory. The Lab's function is to identify, seize, acquire and analyse all electronic devices related to all cyber-enabled offences reported to collect digital evidence which is presented in a court of law for prosecution purposes. The Banking Fraud Investigation Unit (BFIU) investigates fraud complaints from commercial banks, other financial institutions and parastatals and advises the financial industry on fraud prevention and detection strategies.

The Office of the Director of Public Prosecutions – The Office of the Director of Public Prosecutions (ODPP) is the National Prosecuting Authority in Kenya which has been mandated by the Constitution to prosecute all criminal cases in the country.

The National Treasury and Planning – The National Treasury formulates, evaluates and promotes economic and financial policies that facilitate social and economic development in conjunction with other national government entities. The ministry acts as the custodian of the national Public Financial Management regime including the Integrated Financial Management System (IFMIS), an Oracle based Enterprise Resource Planning (ERP) aimed at enhancing accountability and transparency. The system is integrated with Kenya's revenue collection system I-Tax system from Kenya Revenue Authority (KRA) and internet banking from the Central Bank of Kenya (CBK) enabling direct online payments eliminating cash and cheque payments in government.

Ministry of ICT, Innovation and Youth Affairs – The Ministry of Information, Communications and Technology (ICT) has responsibility for formulating, administering, managing and developing Information, Broadcasting and Communication policies and laws that regulate standards and services in the industry. The Ministry is split into two state departments: Broadcasting and Telecommunications as well as the State Department of ICT and Innovation.

The ICT Authority – The Information and Communication Technology (ICT) Authority is a State Corporation under the Ministry of Information Communication and Technology tasked with rationalising and streamlining the management of all Government of Kenya ICT functions. Its broad mandate entails enforcing ICT standards in Government and enhancing the supervision of its electronic communication, a function it executes in close collaboration with the Kenya Bureau of Standards (KEBS) – the State Agency mandated with the development of standards and promotion of standardisation in industry and commerce.

The Department of Information Security therefore develops and implements strategic ICT intelligence security policies, standards, guidelines, plans and procedures for the Government, oversees and enforces ICT security guidelines for Government and is mandated to develop and implement a national Government information security incident reporting & response system.

The National Cyber Command Center (NC3) – The Command Center is a multi-agency entity established to strengthen and coordinate National cybersecurity efforts. It is responsible for spearheading all national cybersecurity matters/programs in Kenya and provides cybersecurity advisory to the government, ensures protection of critical national infrastructure and Kenyans against cyber threats and attacks.

The National Computer and Cyber Crimes Coordination Committee (NC4) – The NC4 is established under the Computer Misuse and Cybercrimes Act, 2018. It comprises of representatives from various government agencies to oversee the security related aspects of the Kenyan cyberspace. The function of the Committee is to coordinate cyber activities and be the central point of contact for all cybersecurity matters including advising the National Security Council on computer and cybercrimes.

Judiciary – The Judiciary is one of the three state organs established under Chapter 10, Article 159 of the Constitution of Kenya with the primary role to exercise judicial authority. The High Court of Kenya has four specialist subject matter divisions including the dedicated Anti-Corruption and Economic Crimes Division. The Division listens to and determines cases with the intention of prevention and punishment of corruption, economic crime and related offences.

Central Bank of Kenya – The Central Bank of Kenya was established by the Central Bank of Kenya Act and is anchored in the Constitution under Article 231.[63] The mandate of the Bank is to formulate and implement monetary policy that promotes price stability, fosters liquidity, solvency and stability of the banking sector, issues currency notes and coins, and provides banking services to the government, commercial banks and other financial institutions.

The SACCO Societies Regulatory Authority (SASRA) – SASRA is the government's principal agency responsible for the supervision and regulation of SACCO Societies in Kenya.[64] Its objectives include licensing, regulation and supervision of Sacco societies to carry out deposit-taking business, make recommendations with regard to business conduct, issue directions regarding measures to improve the management or business methods of the society or to secure or improve compliance with legal requirements. In granting a licence to a SACCO, SASRA requires all saccos to put in place risk management policies and internal control systems.[65] Subject to section 49, it has the power to inspect and

63 Central Bank of Kenya Act, *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/CentralBankofKenyaAct_Cap491.pdf*
Constitution of Kenya, *http://www.kenyalaw.org/lex/actview.xql?actid=Const2010*

64 The Sacco Societies Act 2008, *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/SaccoSocietiesAct_No14of2008.pdf*

65 Sacco Societies (Deposit-Taking Sacco Business) Regulations, 2010,
http://kenyalaw.org:8181/exist/kenyalex/sublegview.xql?subleg=No.%2014%20of%202008

assist any investigative authority regarding matters of suspected fraud or malpractice in Sacco societies either by identification of such matters for referral or at the request of such authority.

Communications Authority – The Communications Authority licences telecommunications operators and service providers in Kenya. It monitors their performance on a continuous basis to ensure that they discharge their licence obligations.[66] The key licensees of the Authority at the Network Facilities Providers (NFP) who establish and operate communication infrastructure using any form of technology, whether fibre, copper, satellite or microwave systems, for purposes of leasing for use by application service providers to provide services. Aside from the Network Facilities Providers (NFP) who provide physical telecommunications infrastructure, the Authority also regulates Application Service Providers[67] and Content Service Providers.[68]

The Competition Authority of Kenya – The Competition Authority (CAK) is tasked with the oversight and advisory role on matters relating to competition and consumer welfare. The core function of its Consumer Protection Department is to investigate complaints relating to false or misleading representations, unconscionable conduct, promoting the creation of consumer bodies and the standards they should adhere to, working with consumer bodies to promote consumer welfare and sensitising consumers about their rights and obligations.[69] The CAK collaborates with other regulators to protect consumers including the Communications Authority of (CA), Central Bank of Kenya (CBK), Insurance Regulatory Authority (IRA) and Kenya Consumer Protection Advisory Committee (KECOPAC).

Kenya Consumer Protection Advisory Committee (KECOPAC) – KECOPAC established under the Consumer Protection Act 2012 has an obligation to ensure relevant action on all aspects relating to consumer protection, policy formulation, creation of awareness, establishment of dispute resolution mechanisms and review of consumer protection directives.[70]

3.2 Private Sector

Banks, Financial Institutions and Microfinance Banks – According to Section 4 of the Banking Act CAP 488, every institution intending to transact banking business, financial business or the business of a mortgage finance company in Kenya shall, before commencing such business, apply in writing to the Central Bank for a licence.[71] The Microfinance Act No. 19 of 2006 provides for the regulation of microfinance banks, i.e. companies licensed to carry on microfinance bank business, licensed by the Central Bank of Kenya.[72] As financial intermediaries, MFBs play a complementary role to commercial banks, as opposed to being competitors, by offering a vital service channel to the significant proportion of the population in Kenya that lacks access to commercial banks. Also licensed as a financial institution are money

66 Kenya Information and Communications Act, 1998 and the Kenya Communications Regulations, 2001

67 Application Service Providers (ASPs) provide any form of service to end users using the infrastructure leased from an NFP licensee. Such services include but are not limited to voice, data, Internet, mobile virtual network operator, vehicle tracking services etc. The services are all communication services except services that are content in nature.

68 Content Service Providers provide content related services to end users who are customers of the application service providers. Content service providers use the infrastructure of Network Facilities providers and the Systems of the Application Service Providers to reach their customers. The services offered by content service providers are of information, entertainment, education, health, social etc nature that can either be text, voice, video clips delivered to a customer's mobile device on request or as subscribed to by the customer.

69 Competition Act, No 12 of 2010 *https://www.cak.go.ke/sites/default/files/Competition_Act_No._2012_of_2010.pdf*

70 Vol.CXXIII-No.161, Vide Kenya Gazette Notice dated 06 August,2021 the Cabinet Secretary for Industrialization, Trade and Enterprise Development appointed 9 members to be members of the Kenya Consumer Protection Advisory Committee, for a period of three (3) years, with effect from the 22nd July, 2021

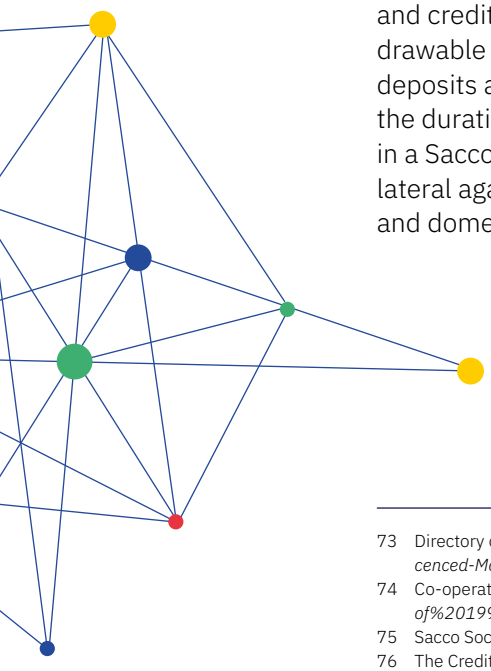
71 Banking Act, *http://www.kenyalaw.org/lex//actview.xql?actid=CAP.%20488#sec_5*

72 Microfinance Act No. 19 of 2006, *http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2019%20of%202006*

remittance providers that enable customers to transfer money within or outside the country.[73]

Cooperative Societies – The objective of a cooperative society is generally to promote the welfare and economic interests of its members or adherence to the principles of Islamic law; and has incorporated in its by-laws the following co-operative principles: voluntary and open membership; democratic member control; economic participation by members; autonomy and independence; education, training and information; cooperation among cooperatives; and concern for community in general.[74]

The Sacco sub sector comprises both Deposit Taking and non-Deposit Taking Saccos. Deposit Taking Saccos (DT Saccos) are licensed and regulated by SASRA while non-Deposit Taking Saccos are supervised by the Commissioner for Co-operatives. SASRA licensed Saccos that have been duly registered under the Cooperative Societies Act. A Sacco society means a savings and credit co-operative society registered under the Co-operative Societies Act Undertaking financial intermediation through receipt of withdraw-able deposits, domestic money transfer services, loans, finance, advances and credit facilities; or receipt of non-withdrawable deposits from members and which deposits are not available for withdrawal for the duration of the membership of a member in a Sacco society and may be used as collateral against borrowings providing finance and domestic money transfer services.[75]



Credit Reference Bureaus and Credit Information Providers – A Credit Reference Bureau (CRB) is an entity licensed by the Central Bank to collect and collate credit information on individuals and businesses from different sources and provide that information upon request mainly by credit providers in the form of a credit report.[76] As of April 2021, there were three duly licensed CRBs.[77] Banks are permitted to disclose any positive or negative information of its customers to the licensed credit reference bureaus, where such information is reasonably required for the discharge of the functions of the banks and the licensed credit reference bureaus.[78]

The Credit Reference Bureau Regulations (2020) allow Credit Reference Bureaus (CRBs) to source for credit information from third parties to enhance their databases, to provide a complete and comprehensive credit history of the borrower. Through this arrangement, CRBs have been able to broaden their databases with data from third-party Credit Information providers (CIPs) after conducting due diligence on the sources and obtaining approval of CBK.

Third-party CIPs are providers of credit information other than commercial banks, microfinance banks and deposit-taking savings and credit co-operative societies which are mandatory subscribers. The Regulations require that customers are protected and a mechanism for handling customer complaints be in place to ensure that customers' complaints or disputes are handled expeditiously.[79]

Payment Service Providers – Payment Service Provider (PSP) as defined in the National Payment Systems Act, 2011 means: a person, company or organisation acting as a provider in relation to sending, receiving, storing or processing of payments or

73 Directory of Licensed Money Remittance Providers, *https://www.centralbank.go.ke/wp-content/uploads/2021/09/Directory-of-Licenced-Money-Remittance-Providers-Sep-2021.pdf*
74 Co-operative Societies Act, No. 12 of 1997, *http://kenyalaw.org:8181/exist/kenyalex/actviewbyid.xql?id=KE/LEG/EN/AR/C/No.%2012%20of%201997#KE/LEG/EN/AR/C/NO.%2012%20OF%201997/sec_4*
75 Sacco Societies Act, 2008, *http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2014%20of%202008*
76 The Credit Reference Bureau Regulations, 2013, *https://www.centralbank.go.ke/images/docs/legislation/CREDIT_REFERENCE_BUREAU_REGULATIONS_2013.pdf*
77 Directory of Licensed CRBs, *https://www.centralbank.go.ke/wp-content/uploads/2021/04/Directory-of-Licensed-CRBs-April-2021.pdf*
78 S. 36A Central Bank of Kenya Act, *https://centralbank.go.ke/images/docs/The_Central_Bank_of_Kenya_Act_1st_January_2014.pdf*
79 Third-Party-Credit-Information-Providers, *https://www.centralbank.go.ke/wp-content/uploads/2021/10/Approved-Third-Party-Credit-Information-Providers-30-September-2021.pdf*

the provision of other services in relation to payment services through any electronic system; or a person, company or organisation which owns, possesses, operates, manages or controls a public switched network for the provision of payment services; or any other person, company or organisation that processes or stores data on behalf of such payment service providers or users of such payment services.

Third Party Service Providers and Vendors – A Third-Party Service Provider is an entity that is not an affiliate of the PSP, provides services to the PSP, and maintains, processes or otherwise is permitted access to confidential information through its provision of services to the PSP. Some of these third party service providers offer cloud computing capabilities, enterprise system functionalities such as Microsoft, Craft Silicon, Oracle, Techinnovar Limited, Cyber Security Africa, Inceptor Kenya, Central Information System International (CISI Kenya), Enovise Cyber Security Company, Crystal Technologies; Information Security Management Consulting, research and Training companies such as Silensec, Serianu, the Africa Cyber Immersion centre (ACIC) support in data recovery such as East Africa Recovery Experts and East African Data Handlers.

Sacco Societies are expected to not engage the services of third-party providers or vendors for its management information systems and infrastructure unless due diligence has been undertaken to assess, among others the providers' cybersecurity measures including cybersecurity audit, monitoring cyber-attacks and the providers' risk management measures. The Authority may also issue guidelines or circulars specifying any other feature that a service provider shall comply with before or prior to being engaged by a Sacco society.[80]

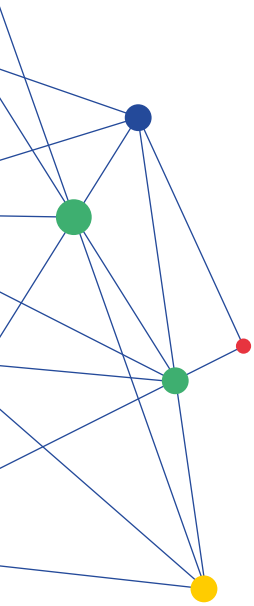
Payments Card Providers – Payment cards include credit, debit and prepaid cards. The banking sector continues to adopt more secure, convenient and safe technology at their cash points to curb insecurity and at the same time enlighten their customers. The retail payment ecosystem in Kenya has undergone significant transformation on account of the adoption of technology and innovations, which has enhanced the digitisation of the economy.

Mobile Money Transfer Service Providers – The mobile phone money transfer operators are authorised as Payment Service Providers under the National Payment System Act 2011 and National Payment System Regulations 2014 under various categories including: Provision of Electronic Retail Transfers, Small Money Issuer, E-Money Issuer and Designation of Payment Instrument. Mobile phone money transfer platforms have moved from the traditional role of transferring money to the provision of banking services to both the banked and unbanked users. Commercial banks have partnered with mobile network operators to enable customers to access their bank accounts through mobile phones. Mobile phones can be used for opening and operating virtual bank accounts and access to traditional banking services like depositing, withdrawing and credit facilities without physical representation to the bank.

Telecommunications Service Providers – Under the telecommunications sub-sector, there are three (3) Tier 1 Network Facilities Providers: Safaricom Limited, Airtel Networks Kenya Limited and Telkom Kenya Limited.[81] This licence allows a licensee to deploy communication infrastructure, using any technology, countrywide with the main difference that it allows for a national spectrum reservation and allocation particularly for the mobile services. All three mobile service providers offer financial services, including, wealth management, savings, insurance and credit, subject to regulatory

80 R 89, Sacco Societies (Non-Deposit-Taking Business) Regulations, 2020 *http://www.parliament.go.ke/sites/default/files/2020-06/Sacco%20Society%20%28Non-Deposit%20Taking%20Business%29%20Regulations%202020%20%282%29-min.pdf*

81 Register of Unified Licensing Framework, October 2021, *www.ca.go.ke/wp-content/uploads/2021/10/Register-of-Unified-Licensing-Framework-Licensees-October-2021.pdf*



approvals. Safaricom PLC for instance identifies its business' key pillars to include, being a 'Financial Services Provider'.[82]

M-PESA is a mobile phone-based money transfer, payments and micro-financing service, launched in 2007 by Vodafone Group and Safaricom. The service allows users to deposit money into an account stored on their cell phones, to send balances using PIN-secured SMS text messages to other users, including sellers of goods and services, and to redeem deposits for regular money. M-PESA not only allows for P2P transfers and withdrawal, but also payment options and connectivity to formal banking and credit access. It has also facilitated international transactions and deepened financial inclusion in the country.

Non-regulated financial intermediaries – Mobile-enabled platforms are increasingly disrupting traditional value chains across the region, which escalated during the pandemic as businesses have been forced to adapt to a world of social distancing where face-to-face interactions are rapidly declining. These platforms – mostly developed by rapidly expanding local tech start-up ecosystems – aim to eliminate inefficiencies in conventional business models, as well as extend the reach of services and provide greater choice to customers.

Some of these players in Kenya include aggregators and electronic payment service providers such as Flutterwave, Interswitch, iPay; money transfer providers, Tap Tap Send, Pesapal, Abacus, Umati Capital, BitSoko, Branch International, Chura, Jambopay, Inuka Pap, Chipper Cash, M-Changa (fundraiser management platform), WorldRemit, Cellulant; digital lenders Tala, Branch etc.

According to the 2021 Digital Trend Report's review of the mobile app landscape (Primarily on Google's Android ecosystem), there has been a greater emphasis on digital experiences – including for financial institutions.[83] Some of these providers lump several financial services together such as Chipper Cash, an African cross-border payments company which offers financial solutions in payments, investing in cryptocurrency and company stock, business solutions for both end users and business enterprises. In social payments, Twitter recently launched its Tips feature, also known as Tip Jar, to allow creators to receive money on its platform integrated with payments platforms, including Chipper, PayPal, Patreon, GoFundMe, Cash App and Venmo, to make it accessible in different regions.[84]

Digital Media and Social Media Platforms – Several bloggers and new age media creators have developed and operate business and technology blogs. Business blogs feature business content like business development, entrepreneurship, start-ups, stocks, investments, banking, finance etc while technology blogs cover technology matters like gadgets, social media, web culture, internet usage, tech start-ups etc. Some of these platforms raise awareness of cybersecurity and end user issues such as the Kenyan Wallstreet,[85] HapaKenya, Tech-ish,[86] Techweez,[87] and CIO Africa.[88]

On Social Media platforms, several users curate content on cybersecurity, financial services as well as technology concerns. According to the Nendo 2021 Digital Trend Report, social media broadly and specifically the juggernaut of apps owned by Meta – Facebook, Messenger, Instagram, and WhatsApp are among the top platforms used by Kenyans with internet access. Twitter continues to grow and maintain a higher-than-usual level of influence.

82 Safaricom 2021 Annual Report, *SAFARICOM PLC Annual Report and Financial Statements 2021*
83 2021 Digital Trends Report, *2021 Digital Trend Report*
84 TechCrunch, *Chipper Cash gets $2B valuation with $150M extension round led by FTX | TechCrunch*
85 Kenyan Wallstreet: Business News, Finance News, Investment *https://kenyanwallstreet.com*
86 Tech-ish, *https://tech-ish.com/*
87 Techweez, *https://techweez.com/*
88 CIO Africa, *https://www.cioafrica.co/*

Active Twitter users and thought leaders have in the past pooled resources to lead user generated campaigns, spark conversation or enhance awareness creation on key issues through hashtags and trending topics. For insurance, Bei ya Ukweli is a group of Kenyan students with a mission to achieve consumer price transparency who regularly reports and updates on commodity prices for the benefit of the Kenyan end user.[89]

3.3 Academia

The Kenya Universities and Colleges Central Placement Service (KUCCPS) is a State Corporation that provides career guidance and selects students for admission to universities, national polytechnics, technical training institutes and other accredited higher learning institutions for Government of Kenya-sponsored programmes. The Service has 301 registered members which offer 21 accredited Computer, IT and Related Courses including a Bachelor of Information Communication Technology, Bachelor of Science (Telecommunication & Inform. Tech), Bachelor of Business Information Technology, Bachelor of Information Technology and Bachelor of Science Computer Science Most Popular Bachelor of Information Science, Bachelor of Science in Computing and Information Systems, Bachelor of Science (Computer Security and Forensics) and Bachelor of Technology (Electrical and Electronic Engineering).

There is only one dedicated course on cybersecurity, the Bachelor of Science (Computer Security and Forensics) programme that is offered in two institutions.[90] In 2020, the ICT Practitioners Bill was reintroduced before the Parliament and faced great opposition from the practitioner's community as most do not have mainstream qualifications such as degrees and diplomas due to the fast-evolving nature of the industry.[91]

3.4 Technical Community

The National Kenya Computer Incident Response Team – The Kenya Information and Communications Act from 1998 mandates the Communications Authority to develop a national cybersecurity management framework through the establishment of a national Computer Incident Response Team (CIRT) in order to mitigate cyber threats and foster a safer Kenyan cyberspace. The National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), is a multi-agency collaboration framework that is responsible for the national coordination of cyber security as well as Kenya's national point of contact on cyber security matters.

ISACA – ISACA Kenya is a not-for-profit, non-union association of professionals in the IT-related industry founded in Kenya in December 1999 by a group of volunteers. ISACA membership provides access into the world's largest global organisation for empowering IS/IT audit, control, security, cybersecurity and governance professionals to succeed in any industry. ISACA collaborates with other professional non-profit and standard setting organisations to address and respond to issues of mutual importance, provide professional guidance and to offer training and professional development opportunities. Such cooperation is aimed at both a global and local level.

3.5 Civil Society and Sector Organisations

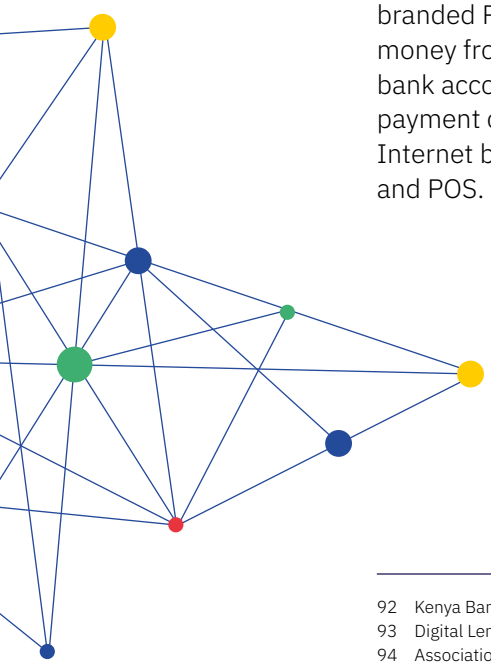
Financial institutions have not been sensitive to dynamic needs of financial services consumers raising consumer protection and rights concerns such as transparency in pricing and marketing practises, hidden charges, alternative dispute resolution mechanisms, complaints grievances handling arrangements, protection against over indebted-

89 Bei Ya Ukweli, *https://twitter.com/beiyaukweli*
90 KUCCPS Programme Cutoffs, *https://statics.kuccps.net/uploads/globalFiles/Programme_Cut-offs.pdf*
91 Report of the Information Communication Technology Practitioners Bill, Nox.38 of 2020, *http://www.parliament.go.ke/sites/default/files/2021-08/Report%20of%20the%20Information%20Communication%20Technology%20Practitioners%20Bill%2C%20Nox.38%20of%202020_0.pdf*

ness and fair debt collection practises, and fostering financial literacy, among others. There are several consumer organisations in Kenya including the Consumer Unit Trust Society (CUTS), the Consumer Federation of Kenya (COFEK), the Consumer International Network (CIN), the Kenya Consumer Organisation (KCO), the Insurance Consumers Federation of Kenya (ICFK), the Association of Insurance Consumers of Kenya (AICK) and the Information Communication Technology Consumers Association of Kenya.

Kenya Bankers Association (KBA) – The Kenya Bankers Association is registered as an Industry Association by the Registrar of Trade Unions and is the umbrella body of the institutions licensed and regulated by the CBK with a current membership of 47 financial institutions.[92] It seeks to reinforce a reputable and professional banking sector with several committees including the Bank Fraud & Risk Committee which comprises the Bank Fraud and Security Sub Committee, the Bank Forensics Sub Committee and the Bank IT Systems, Risk & Security Sub Committee.

In embracing innovation and interoperability, the Kenya Bankers Association established the Integrated Payments Service Limited (IPSL)in 2012 under the National Payment System (NPS) Act to address the challenge of integrating retail payments in the country. The inter-banking money transfer service, branded PesaLink, allows customers to send money from one bank account to another bank account in real time on all banks' retail payment channels including mobile, ATM, Internet banking, Agency, Bank branches and POS.



Digital Lenders Association of Kenya (DLAK) is the umbrella body of digital lenders in Kenya. DLAK was formed in March 2019 with the objective of bringing together Digital Lenders and associated players to promote responsible lending practises and help the ecosystem grow. Currently the association has 22 members registered under its leadership.[93]

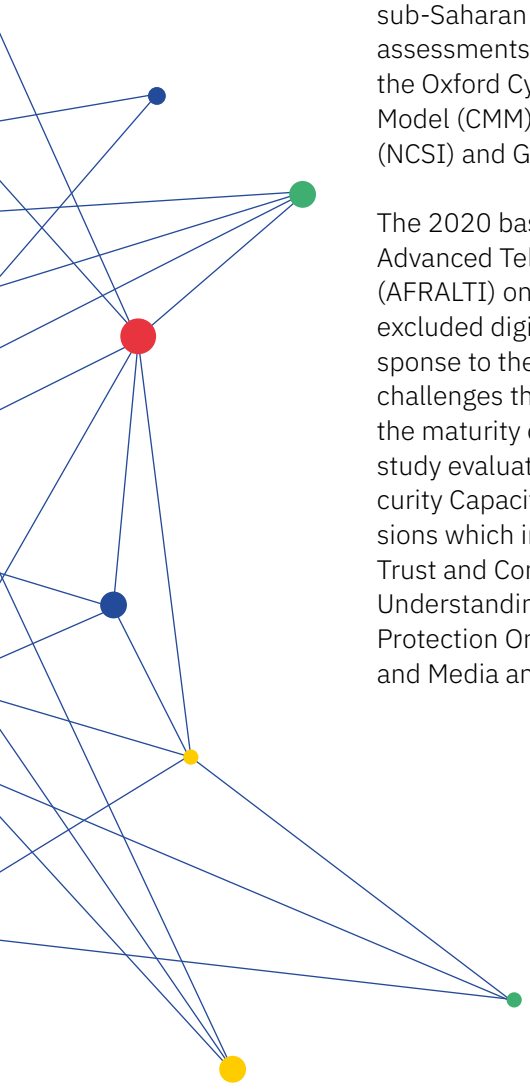
Association of FinTechs in Kenya (AFIK) was founded in 2021 by a team of experienced professionals within the fintech space, the organisation was established to have a single platform for innovation in Kenya. The association seeks to foster National, Regional and International co-operation in matters dealing with digital innovation, influence policy making, raise awareness on the benefits of adopting digital solutions to the public and mitigate common challenges faced by member companies in the macroenvironment they are in. The Association currently has 123 members.[94]

The Kenyan FinTech Association (FINTAK) is the first not-for-profit organisation representing leading FinTech companies of all sizes, within Kenya aiming to serve as a resource and forum for education, information sharing, and networking between companies, policymakers, and the general public.[95] It seeks to promote, communicate and develop cooperation and dialogue between Fintech companies within Kenya, advocate and represent the interests of its members at the policy level as well as lead Fintech companies in delivering comprehensive, innovative and understandable financial services products for all Kenyans. Moreover, it aims to foster sound tech regulation that is beneficial for the overall Kenyan financial market making consumers see the advantages of technology for finance.

92 Kenya Bankers Association (KBA), *https://www.kba.co.ke/members.php*
93 Digital Lenders Association of Kenya (DLAK), *https://www.dlak.co.ke/*
94 Association of FinTechs in Kenya (AFIK), *https://afik.or.ke/*
95 Kenyan FinTech Association (FINTAK), *https://fin-tech.co.ke/*

4 Cyber threats

This section identifies the cyber security threats in Kenya and provides security statistics from different sources.



4.1 National Cybersecurity Assessments

This section provides a comparative of Kenya's position against some countries within sub-Saharan Africa based on recent national assessments of cyber security status such as the Oxford Cybersecurity Capacity Maturity Model (CMM), National Cyber Security Index (NCSI) and Global Cybersecurity Index (GCI).

The 2020 baseline study by the African Advanced Telecommunication Institute (AFRALTI) on cyber hygiene for digitally excluded digital populations in Kenya in response to the COVID-19 pandemic identified challenges that if addressed could deepen the maturity of cybersecurity in Kenya. The study evaluation was based on the Cybersecurity Capacity Maturity Model (CMM) dimensions which include Cybersecurity mindset, Trust and Confidence on the Internet, User Understanding of Personal Information Protection Online, Reporting Mechanisms and Media and social media. The assessments are based on five distinct stages of maturity: start-up, formative, established, strategic, dynamic, which define the degree to which a country has progressed in relation to a certain Factor or Aspect of cybersecurity capacity.[96]

On the cybersecurity mindset, the following were the outcomes: government, private sector and users (established). On user trust and confidence in the internet, the following were the assessments: user trust in e-government services (formative), user trust in e-commerce services (established), user understanding of personal information protection online (established), reporting mechanism (formative), and media and social media (established). On cybersecurity education and training, the following were the assessments: awareness raising programmes (formative), awareness raising (established), and the framework for provision of education (established), administration (formative), and framework for professional development (formative).

The AFRALTI study also identified challenges raised by stakeholders that if addressed could deepen the maturity of cybersecurity in the country. These included: for instance, the resistance to change as digitisation is often considered too expensive; as well as limited understanding of cybersecurity culture and its value. Hence, this derives the difficulty of getting stakeholder buy-in, a shortage of cybersecurity skills and limited profession-

96 Global Cyber Security Capacity Centre, *https://gcscc.ox.ac.uk/the-cmm*

als with hands on skills. Moreover, a lack of strategic partnerships between government, learning institutions and professional bodies hinder progress; and lastly, few programmes targeting and reaching out to excluded digital populations, including persons with disabilities and developing content that is relevant for these groups.

An analysis of Kenya's CMM assessment by KPMG revealed generally that CMM dimensions such as user cyber security mindset; user trust and confidence on the internet; user trust in e-government services; user understanding of personal information protection online; reporting mechanisms; media and social media; and the provision of education, were all assessed as being in the formative stages. Simply stated, a formative rating indicates that some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new. These dimensions touch on aspects that relate to individual users. Therefore, it is crucial to prioritise key measures for the marginalised like attitudes, beliefs and values that motivate them to continually act in ways that secure their environment, and understanding of personal information protection online, education, and reporting mechanisms.

The National Cyber Security Index (NCSI) measures the level of cyber security focusing on the organisational, regulative and technical aspects of cybersecurity at a national level and conducts country cybersecurity maturity level assessments. The index also identifies the main fields of priority that need to be tackled to improve a country's cyber security status and provides an overview of countries' preparedness to prevent and fight cyber-attacks and crimes. Analysing these fields helps governments to identify the gaps in policies and strategies that should be put in place to improve a country's cybersecurity. According to the National Cybersecurity Index, Kenya is ranked 64th globally ahead of Mauritius 67th, and South Africa 84th but behind Egypt 48th, Zambia 49th, Uganda 54th, Benin 53rd, and Nigeria 55th. Kenya scores poorly in contribution to global cyber security, protection of digital services, protection of essential services, cyber crisis management, and military cyber operations.[97]

The Global Cybersecurity Index (GCI) by the International Telecommunication Union (ITU) measures the commitment of 194 countries to cybersecurity to help them identify areas of improvement and encourage countries to take action within the field through raising awareness on the state of cybersecurity worldwide. The index measures legal, technical, organisational, capacity development and cooperative measures. Kenya was 5th in Africa with 81.7 in the ITU's 2020 global cybersecurity index. Other African countries ahead of Kenya in the sub-Saharan region are Mauritius 96.89, Tanzania 90.58, Ghana 86.69, and Nigeria 84.76.[98]

From the foregoing, it is apparent that Kenya ranks well as compared to its immediate neighbours, however, the country still falls behind globally, and more importantly, in certain critical areas identified by the various assessments. Unfortunately, across all the indices, some of the indicators used to assess Kenya are not up-to-date, or not populated, likely due to the challenges in accessing the statistics, or due to the information not being provided by Kenya.

Kenya was

5th.

in Africa in the ITU's 2020 global cybersecurity index

97 National Cyber Security Index, *https://www.ncsi.ega.ee/*
98 ITU Global Cybersecurity Index 2020, *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf*

According to the KE-CIRT statistics for the second quarter of 2021, ransomware, malware, and phishing attacks are the most common cybersecurity risks.

4.2 Cyberthreats in Kenya

In the past three years, Kenya has seen cyber threats continue to increase. The total threats detected by the KE-CIRT[99] have grown from 23 million in 2018 to 110 million in 2020. The KE-CIRT is responsible for national-level cyber incident detection and response. It issues alerts and advisories on cyber threats[100] and best practice security guide for institutions and the general public, and quarterly reports on the threat landscape.[101] The increase in cyber threats that can be attributed to targeted attacks such as at Internet of Things (IoT) devices, increased activity by organised cybercrime groups, and adoption of more sophisticated tools by ransomware gangs. One other reason for the increase in attacks is that the number of broadband subscriptions went up from 15.4 million in 2016 to 22.5 million in 2020 meaning there is an increase in devices, and overall, more people are using the internet.

According to the KE-CIRT statistics for the second quarter of 2021, ransomware, malware, and phishing attacks are the most common cybersecurity risks. Malware constitutes 59.5 percent, botnet and Distributed Denial of Service (DDoS) assaults are at 29.1 percent, and web application attacks are the most frequent attack mechanisms at 6.6 percent.[102] In 2020, KE-CIRT issued 72,515 cyber threat advisories from 48,664 the previous year. The advisories were classified as system vulnerabilities (60,593), malware (7,718), DDOS/Botnet (1,829), web application attacks (687), online abuse (196), impersonation (585), Ransomware (66), phishing (388), online fraud (192), child abuse (28).

This, again, is an upward trend which can be attributed to the rise in impersonation, online fraud, and online abuse cases arising from increased Internet access and use. Data breaches, theft of proprietary information, financial damage, reputational loss, equipment destruction, distributed denial of service, illegal access to vital systems, and theft of personally identifiable Information are all consequences of these attacks. As part of the mitigation measures, the KE-CIRT conducted 39 digital forensics, 95 mobile forensics, 5 network forensics, and issued 94 cybersecurity best practice guides.

At the institutional and policy levels, the Kenyan cybersecurity landscape witnessed some changes recently with the launch in October 2021 of the National Computer and Cyber Crimes Coordination Committee (NC4) envisaged in the Computer Misuse and Cybercrimes Act, 2018.[103] The NC4 is now tasked with strengthening the detection, investigation, and prosecution of cybercrimes. Notably, the KE-CIRT report does not provide any sector specific statistics on cyber threats. For example, there is no classification on how the threats affected the banking, manufacturing, transport, or healthcare sector.

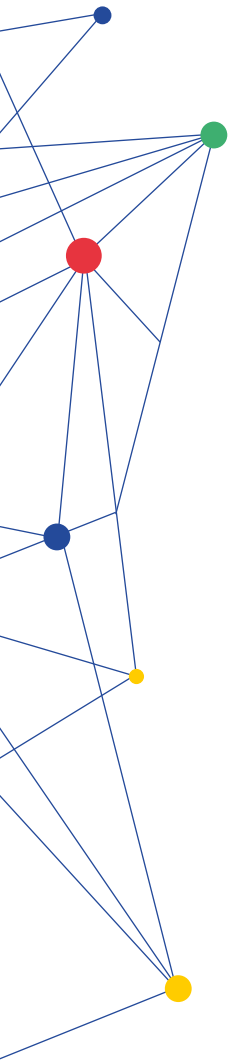
110 Mio.

threats detected by the KE-CIRT in 2020

99 *https://www.ca.go.ke/wp-content/uploads/2021/05/Annual-Report-for-Financial-Year-2019-2020.pdf*
100 KE-CIRT Alerts and Advisories, *https://ke-cirt.go.ke/alerts-advisories/*
101 KE-CIRT Quarterly reports, *https://ke-cirt.go.ke/quarterly-reports/*
102 National Ke-CIRT/CC. Cybersecurity Report. April to June 2021, *https://ke-cirt.go.ke/wp-content/uploads/2021/08/Quarter-4-FY-2020_21-National-KE-CIRT_CC-Cybersecurity-Report-Public-Version.pdf*
103 Computer Misuse and Cybercrimes Act, 2018. *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf*

Table 1: KE-CIRT Cyber attacks detected in Kenya

Cyber attack vector	2017/2018	2018/2019	2019/2020
Malware	16,306,547	40,893,141	101,651,143
BotNet/DDOS	3,756,334	4,852,022	1,475,537
Web Application Attacks	3,743,638	6,109,184	7,662,793
System vulnerability threats	6,158	47,913	108,596
Online Abuse	2,927	458	196
Online Impersonation	368	568	585
Advisories issued	7,180	48,664	72,515
Total cyber threat events	**23,815,972**	**51,903,286**	**110,898,850**



The KE-CIRT noted an increase in Internet of Things devices connected which may have led to the increase of threats, and increased activity by organised cybercrime groups, and adoption of more sophisticated tools by ransomware criminals. The KE-CIRT also noted an increase in attacks to critical systems and services, an increase in e-skimming and credit card fraud, exploits of mobile application vulnerabilities, targeted attacks at cloud-based services and unsecured infrastructure. There was also an increase in the adoption of botnet and Distributed Denial of Service (DDoS) attack techniques by cybercriminals. E-skimming involves infecting e-commerce platforms with malicious software to intercept shoppers' banking details. The captured details are then sold in the black market or used to make fraudulent purchases.

Serianu, a cybersecurity firm based in Nairobi, in their 2020/2021 Sacco cybersecurity report lists threat vector indicators that financial Saccos should prioritise. These are malware, phishing email, rogue devices and software, and malicious insiders. The vector indicators lead to threats like database compromise, transaction manipulation, customer data manipulation, man-in-the-middle attack, GSM compromise, and API compromise. Serianu notes that cybersecurity programs should be modelled around the risks, vulnerabilities, and threat indicators which are the inputs of successful enterprise cybersecurity operations programs.

Further, Serianu[104] notes that the finance sector (banking, Micro Finance Institutions, and Saccos) lists fraud as the biggest threat. The threats affect the ATM infrastructure, mobile banking infrastructure, debit and credit card systems, and third parties and vendors. They also suffer from sabotage and ransomware compromising their identity management systems (Active Directory). The emerging threats in Kenya are organised crime, exporting cyber criminals to the East African region, cyber criminals moving from financial sector to other areas, social media related scams, API integration weaknesses, ATM attacks, third party attacks, cloud penetrated attacks, crypto mining on local systems, and ransomware and end user system hijacking. The manufacturing, insurance, healthcare sectors and government also face fraud in their payment systems, storage or document management systems, identity management systems (Active Directory), and SCADA systems. Email systems also face phishing threats.

104 Africa Cybersecurity Report Kenya, 2019/2020, *https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf*

4.3 Trends in the Region

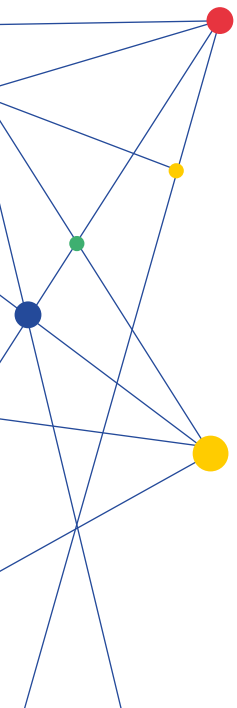
This section highlights several trends in the region. The Global Forum for Cyber Expertise (GFCE) in their "cybercrime & cyber security trends in Africa" report categorises Cybersecurity threats[105] as Social Engineering (scams, threats, fake apps and plugins, compromised apps, business email compromise), Attacks, Malware (ransomware, botnets, crypto jacking), Spam, Phishing (and phishing hosts), Bots, Command and Control servers. Specific threats for financial services are listed as account takeovers, market manipulation and authorised trading, ATM skimming, e-banking and Mobile banking exploitation, Insider access, Supply chain infiltration – e.g malware on software or hardware, and critical infrastructure disruption e.g disabling internet, recovery centres, servers.

The GFCE report lists Africa's top source of attacks with South Africa leading with 314,880 attacks representing 25 percent for the African continent, followed by Egypt (12 %), Kenya (9 %), and Nigeria (7 %).

The GFCE report notes that many scams rely on the poor security habits of the general public to succeed, but misconfigured systems and poor website security still exposes users to harm. Use of sophisticated social engineering con-tricks to bypass security systems designed to safeguard users is quite too common. The scammers trick users to go through legitimate login processes, or password reset processes, therefore ending by taking over bank accounts, emails, or mobile money accounts. With the increase of social media users across Africa, for example Facebook has 256 million users (18.5 %) as of 2021,[106] it only means these types of social engineering attacks will continue to increase. Social media, scams, and email threats can come in the form of fake apps, fake plugins, victims manually sharing scams like videos or messages, fake offerings where users join fake events or groups, or likejacking where users click on websites that install malware.

The GFCE report lists Africa's top source of attacks with South Africa leading with 314,880 attacks representing 25 percent for the African continent, followed by Egypt (12 %), Kenya (9 %), and Nigeria (7 %). For malware, South Africa leads with 1.7 million (20 %), Tunisia (14 %), Kenya (8 %), Nigeria (6 %). With respect to spam, South Africa led with (24 %), followed by Tunisia (14 %), Egypt (7 %), and Kenya (7 %). As regards phishing, South Africa led with 74 percent, followed by Morocco (5 %), Egypt (3 %), and Kenya (3 %). As for Bots, Egypt led with 48 percent, followed by Algeria (15 %), Tunisia (6 %), and South Africa (5 %). Finally, with respect to Command and Control (C&C) servers, Ivory Coast led with 45 percent, followed by South Africa (19 %), Morocco (17 %), and Egypt (5 %).

These statistics are a bit old, but they represent the general trend across the continent. South Africa leads in the frequency of different types of threats, with Kenya and Egypt also featuring in the top attacks. This does not mean other countries like Nigeria do not have just as many attacks, but that their tracking and measurements is still nascent. A 2020 report by Trend Micro still puts South Africa ahead in threat detections with 230 million threat detections in total, while Kenya had 72 million and Morocco 71 million. In South Africa, 219 million detections were related to email threats. South Africa also had the highest targeted ransomware and business email compromise attempts.



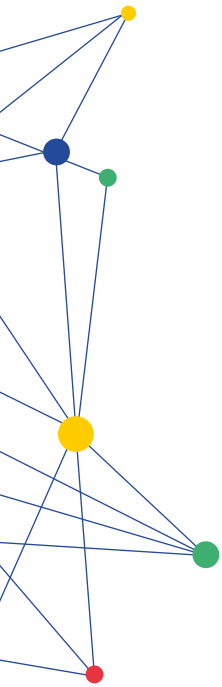
105 Cyber crime & security trends in Africa, *https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf*

106 Africa Internet users, 2021 Population and Facebook Statistics, *https://www.internetworldstats.com/stats1.htm*

Table 2: GFCE Incident Count

Country	Attacks	Malware	Phishing hosts	Bots	C&C servers
South Africa	314,880 (25 %)	1,716,308 (20 %)	4,621 (74 %)	768,800 (5 %)	391 (19 %)
Egypt	149,685 (12 %)	400,679 (5 %)	184 (3 %)	6,778,893 (48 %)	99 (5 %)
Kenya	106,265 (9 %)	668,194 (8 %)	160 (3 %)	435,032 (3 %)	21 (1 %)
Nigeria	89,100 (7 %)	469,018 (6 %)	136 (2 %)	488,416 (3 %)	
Algeria	60,381 (5 %)	304,114 (4 %)	48 (1 %)	2,117,402 (15 %)	98 (5 %)
Morocco	34,464 (3 %)		319 (5 %)	768,800 (4 %)	345 (17 %)
Tunisia	32,187 (3 %)	1,166,774 (14 %)	112 (2 %)	798,121 (5 %)	29 (1 %)

* Ivory Coast leads in C&C servers with 910 (45 %).



The table above summarises the GFCE Incident count top sources for attacks, malware, phishing hosts, bots and command and control servers in Africa in 2016.

Interpol, in its African Cyber Threat Assessment report 2021,[107] identified the top five threats in Africa as online scams, digital extortion, business email compromise, ransomware, and botnets. Interpol notes that criminals take advantage of variations in law enforcement capabilities across physical borders to continue with cyber-attack activities. African countries have reported a sharp increase in the number of online banking scams, including instances of banking and credit card fraud. Online scams are also the highest reported cyberthreat to law enforcement agencies in Africa. The COVID-19 pandemic has contributed to the increase in business email compromise threat that targets businesses and organisations that rely heavily on wire transfer transactions.

61%

more than of companies affected by ransomware in 2020

Ransomware affecting critical infrastructure including healthcare and maritime sector is expanding across the African continent with more than 61 percent of companies affected by ransomware in 2020. The number of botnets where compromised machines are used as a tool to automate large-scale campaigns such as DDoS attacks, phishing, and malware distribution detected in Africa was around 50,000 with a monthly average detection of 3,900. Interpol identified the most common modus operandi for digital extortion as being where threat actors rent Virtual Private Servers (VPS) with an email service to launch bulk extortion emails. Within these digital extortion emails, threat actors often claim to have compromised the security of the victims' computers, files or history.

The threat landscape in Kenya is changing for various reasons. One is the maturity of the KE-CIRT which can now detect, analyse and categorise many threats. The KE-CIRT has also increased its incident handling and response to other threats including ransomware, phishing, online fraud, child abuse, and it has expanded its scope to include digital, mobile and network forensics and additionally, issuing cybersecurity best practice guides. Further, there has been a significant increase in internet penetration, accessibility of computing devices coupled with heightened

107 Interpol identifies top cyberthreats in Africa, *https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa*

use of digital payments, which correlates with the rise of cyber threats. Lastly, private sector-led cyber threat detection command centres such as by Serianu Limited, have been established and are enhancing the digital resilience of their clients in the financial services sector.

4.4 Cybersecurity Challenges

This section reviews the main cybersecurity challenges within the financial services sector.

Loss of Funds due to Cyber-Attacks – According to a report by the cyber-security and business consulting firm Serianu Limited, Kenya lost USD 295 million to cybercrime in 2018. The report noted that financial institutions such as savings and credit cooperative societies, banks, financial services integrators, betting firms and Kenya's government had lost money due to the general increase of cyber-related attacks.[108] Another study assessing the cybersecurity environment of 148 banks in Sub-Saharan Africa (SSA) noted that 85 percent of the banks had experienced cyberattacks and had, on average, incurred losses of USD 770,000 with a single malware-infected computer costing USD 9,707.[109] These figures are conservatively estimated, and the real costs could be higher.

Kenya lost

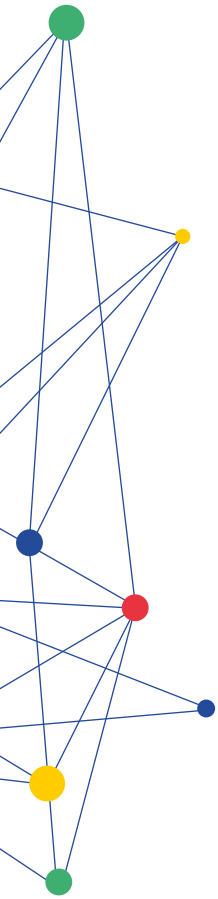
$ 295 Mio.

to cybercrime in 2018

Limited data on breaches – As the costs of cybercrime rise, an emerging challenge is the limited data on cybersecurity related breaches across different sectors. It is difficult to get data on cyber-attacks and data breaches in the financial sector largely due to the fact that previously, there was no requirement on financial institutions to report on incidents of breaches or the losses incurred. However, the Central Bank of Kenya now requires financial entities to document and report on cybersecurity events and related incident response activities. The incident response plan for the entities should address external and internal communications as well as information sharing. They are also required to respond to, contain and be able to rapidly recover from disruptions caused by cyber incidents, thereby strengthening their cyber resilience. The entities should have the capability of operating critical business functions in the face of attacks and while continuously enhancing cyber resilience.[110]

However, the data is not shared publicly. This data sharing should go further by making the breaches public and the steps they take to contain and prevent future breaches, even if it is in a redacted form to safeguard integrity of the affected institutions, and not jeopardise prosecution. For instance, the think tank Carnegie Endowment for International Peace keeps a timeline of cyber incidents Involving financial institutions.[111] The timeline does not cover every single incident but provides insight into key trends and how the threat landscape is evolving over time. The last incident recorded by this database for Kenya was in 2018. There is a need for a local Kenyan organisation to keep a detailed financial institutions incident database.

108 Is Kenya the new playground for cyber criminals? *https://enactafrica.org/research/trend-reports/is-kenya-the-new-playground-for-cyber-criminals*
109 Unveiling the cost of cybercrime in Africa, *https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html*
110 Guidelines on Cybersecurity for Payment Service Providers, *https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf*
111 Timeline of Cyber Incidents Involving Financial Institutions, *https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline*



Few skilled staff and awareness – The Central Bank of Kenya (CBK)[112] noted that increased cyber security risk was a top challenge faced by financial institutions regarding product innovation with 35 percent of banks listing this a high risk. CBK is leading in the development of minimum standards for supervision of cybersecurity in the East African Community region. CBK is ensuring enhanced skills for its staff to be able to respond to evolving digital financial services risks with a focus on cyber resilience. This is because cyber-attacks rely on weaknesses in the human element. Financial institutions are advised to adopt measures such as enhanced cybersecurity awareness through employee training programs, improved risk management and updated business continuity and incident response plans.

Banks need to assess cloud usage related risks and ensure appropriate mitigation measures like investing in security preparedness to enhance their cyber resilience programs in order to mitigate cloud-based cyber-attacks. Kenya Bankers Association conducts regular campaigns called #KaaChonjo[113] on safety tips to protect consumers of financial services from fraud. This includes security tips on text and email scams, the use of strong passwords and changing passwords often, PIN use, legitimate places to get help and discouraging using public computers like cyber cafes for banking tasks.

Wide use of pirated software – The Kenya Bankers Association (KBA)[114] notes, as financial systems become more digitised, there is a need to constantly update security systems to ward off sophisticated fraudsters and respond to cybersecurity challenges. KBA notes that it works with banks to review best practises in identifying fraud, assessing the impact and escalating the information across the industry while tightening response times. However, this may be challenging to achieve because of the wide use of pirated software, and malicious software on mobile apps in Apple's App Store[115] and Android's Play Store.

With Kenya ranking among the top 20 pirating countries,[116] the hidden cost of using pirated software is the likelihood of encountering nasty, unwanted code, either in the software itself, via code that can get downloaded or installed along with it. The malware is created by criminal organisations with illegal financial gain, data theft, espionage, or other mayhem in mind. Consumers and enterprises have a 33 percent chance of encountering malware when they obtain and install pirated software. A research by IDC research estimates that enterprises will spend USD 491 billion because of malware associated with pirated software.[117]

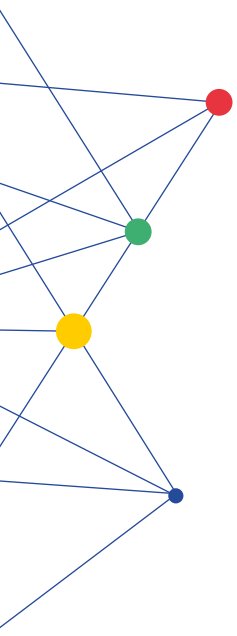
Funding – Availability of clean free alternative software (like open-source software) to pirated software, and proper funding of ICT departments is essential to ensure users are protected from malicious actors. However, cybersecurity is considered to be a luxury and not a necessity in many developing economies. Its importance has not yet been sufficiently appreciated or acknowledged. Cybersecurity budgets in many organisations are reported to be less than 1 percent and many organisations had a zero-budget allocated to cybersecurity.[118] It is therefore important that more resources are directed towards hiring and retention of talent, knowledge and capacity building, and an upgrade of infrastructure – tools and software, as well as invested in cybersecurity strategies.

112 Bank supervision annual report 2020, *https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/468154612_2020%20Annual%20Report.pdf*
113 ATM Safety Awareness, *https://www.kba.co.ke/atm_safety_campaign.php*
114 2019 Kenya Banking Industry shared value report, *https://www.kba.co.ke/downloads/The%20Kenya%20Banking%20Industry%20Shared%20Value%20Report%202019.pdf*
115 How malware gets into the App Store and why Apple can't stop that, *https://habr.com/en/post/580272/*
116 Global piracy study, *https://www.bsa.org/files/reports/IDC_GlobalPiracyStudy_2004.pdf*
117 The Link between Pirated Software and Cybersecurity Breaches, *https://blogs.microsoft.com/uploads/2016/04/IDCNUSFinalResearch.pdf*
118 Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Basingstoke, U.K: Palgrave Macmillan: Houndmills

Prosecution capacity – Several East African hackers including Kenyans linked to bank hacking were arrested in Rwanda in 2021 and handed long prison terms.[119] This criminal gang was already known by security authorities in Kenya after terrorising the banking sector for many years. One criminal group had been founded by a former employee of Kenya's security organs. Despite several arrests and arraignment in Kenya, the hacking gangs were never successfully prosecuted.[120] There is a lack of prosecution capacity in Kenya with several high-profile cybersecurity cases dragging on for many years without being concluded or terminated without prosecution.

Managing evidence – There is also the challenge of safeguarding and securing evidence and ensuring proper chain of custody of evidence to ensure successful prosecution. Prosecuting organs should have adequate training on handling digital evidence and making it admissible in a court of law. Banks are known to avoid negative publicity in case of successful cyber-attacks, and in some cases, may not want to avail evidence to security organs for successful prosecution.

Information Security Gaps – Many cybersecurity threats are due to data breaches when their data falls on the wrong hands, or when organisations have challenges in handling user data. Kenya enacted the data protection law in 2019[121] which requires organisations to securely store the data they collect, inform users why their data is being collected, for what purpose, how long the data will be held, and provision for data subjects to request their data to be deleted. Once the Office of the Data Protection Commissioner is fully operational and prosecutions for data abuse start rolling down the judicial system, we should see organisations start handling data they collect from consumers more responsibly.



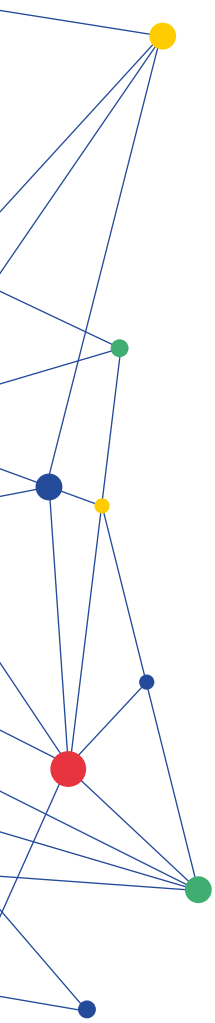
Finally, organisations, especially financial institutions need a clear strategy to manage, improve, and appraise their processes. Using a risk-based approach to cybersecurity (like using the Capability Maturity Model Integration – CMMI model) can be instrumental in addressing cybersecurity challenges as organisations will be able to evaluate their biggest threats, assess vulnerabilities, and reserve resources for those threats. Other frameworks like COBIT by ISACA could also enable organisations to strengthen their IT management and governance. However, little data is available in the region on implementation of well-known standards that can transform local organisations into better managed institutions. This is certainly another gap that needs to be filled in order for the Kenyan cybersecurity landscape to mature.

In conclusion, the study observes that there is increased access, use and adoption of ICTs in the country, which are facilitating the digital payments in the country, and whose value continues to grow as e-commerce becomes more mainstream. Likewise, there is progress in the development of the legal, institutional and regulatory frameworks to promote cybersecurity within the financial services sector, in order to ensure secure digital transactions, even as the stakeholders within the sector increase. The rise of digital payments has also seen an increase in cyber threats targeting the financial sector which continues to face challenges in detection, reporting, responding and preventing cyber-attacks given the level of awareness, capacity, skills and investments to promote digital resilience among the key stakeholders. Moving forward, it will be important for all stakeholders concerned to collectively address the challenges and bottlenecks to ensure secure digital payments and effective responses to the emerging and growing cyber threats in the country, including through human-centric approaches.

119 Rwanda jails 8 Kenyans in Equity Bank hacking case, *https://www.businessdailyafrica.com/bd/economy/rwanda-jails-8-kenyans-equity-bank-hacking-case-3463792*
120 East Africa: How Rwanda Stopped Kenyan Cybergang, *https://allafrica.com/stories/202107250051.html*
121 The Data Protection Act, *http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf*

5 Recommendations

This study makes the following recommendations to the government, private sector, civil society and international development partners.



Government

- Promote a human-centred and multi-stakeholder approach in the implementation of cybersecurity strategies.
- Review the composition of the NC4, and co-opt non-governmental stakeholders to ensure better coordination, information sharing and responses.
- Review the outdated cybersecurity strategy.
- Develop a national cybersecurity policy.
- Develop and implement in collaboration with civil society and other relevant stakeholders, a national cyber hygiene programme targeting users of financial services.
- Promote the establishment of a specific finance sector CIRT in order to promote better coordination, information sharing and responses to cyber incidents.
- Enhance cybercrime information sharing, intelligence, joint cooperation between regional actors in the detection and responses to cyber incidents and the prevention of cybercrimes.
- Build capacity and capabilities for all relevant stakeholders from academia, business, government, media and civil society to promote human-centric cybersecurity.
- Invest in building the capacity of law enforcement, including the police, prosecution and judiciaries to enable them to investigate, prosecute and determine cases on cybercrime.
- Amend the Computer Misuse and Cybercrimes Act to provide a framework for banks and financial institutions to report on incidents, ensure internal cybersecurity frameworks and policies, implement information security protocols, and to create awareness for their customers on possible data and cyber breaches.
- Regularly conduct national cybersecurity assessments based on international standards such as the Oxford CMM, Estonia's National Cyber Security Index (NCIS), and the ITU's Global Cybersecurity Index, and commit to provide updated information to these bodies.

Private Sector

- Invest resources towards hiring and retention of skilled personnel, knowledge and capacity building, and an upgrade of infrastructure, tools and software, as well as in cybersecurity strategies to enable organisations in the financial sector to detect, deter and respond to cyber threats.

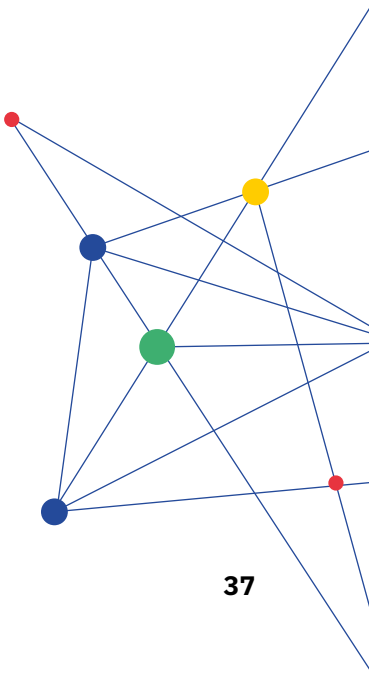
- Develop cyber hygiene programmes and messaging targeted at users of digital financial products and services.
- Ensure compliance with data protection laws and implement adequate information security measures to all services offered to customers and ensure 'security by design' for all applications and services supplied through digital platforms.
- Collaborate with government and civil society government and civil society to promote effective cyber security programmes.
- Do away with the culture of secrecy and embrace more transparency on data breaches, and what companies and firms including telcos and banks, do with the users' data to avoid commercialization of data. This will enhance trust and inspire confidence in the users.
- Collaboration between the banks and regulators, on handling incidents. Consider cooperation with the wider government network, Central Bank, incident response teams.
- For International banks with a local presence, there is a need to report to the parent company, for example on incidents of cyber-attacks.

Civil Society

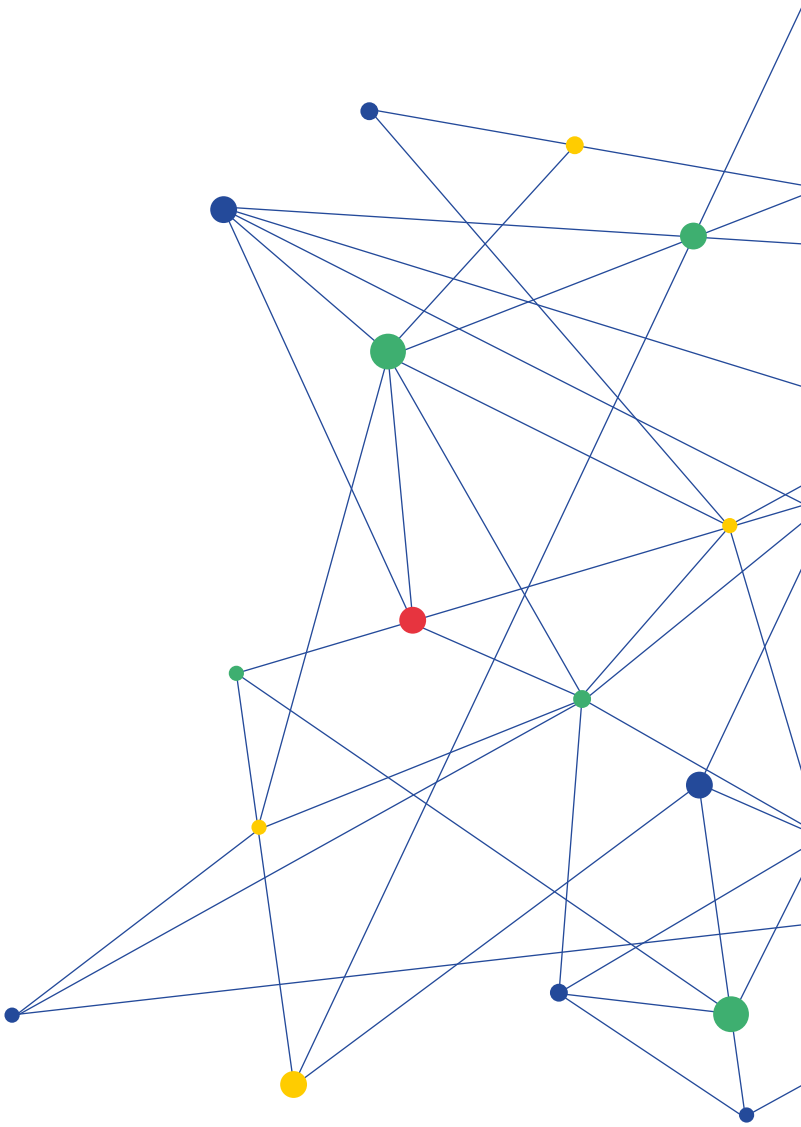
- Develop cyber hygiene programmes and messaging targeted at the public.
- Monitor and report on the effectiveness measures put in place by the government and the financial sector with more focus on human centric approaches to ensure the security of customer data.
- Collaborate with other stakeholders such as media and technical experts to promote effective cyber security programmes and disseminate information.
- Engage national policy and law-making institutions at the national and regional level to incorporate a human rights perspective in cyber laws.

International Development Partners

- Promote a human-centred and multi-stakeholder approach in the implementation of cybersecurity strategies.
- Support civil society organisations to conduct research, advocacy and training for the public, in addition to monitoring measures put in place by the government and the financial sector.
- Collaborate with other stakeholders to promote effective national cyber security programmes benchmarked on international standards.
- Invest in capacity building programmes, information sharing, knowledge and technology transfer, and international cooperation to strengthen the synergies, and capabilities between global and national actors including academia, business, government, media and civil society.
- Support the participation of stakeholders in regional and international discussions on cybersecurity, including advancing human-centric approaches in the efforts towards the development of a global Cybercrime Treaty at the United Nations.



www.giz.de



giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Trust4Cyber

DIGITAL TRANSFORMATION CENTER KENYA

KICTANet The Power of Communities