GOVERNMENT of KENYA

CYBERSECURITY STRATEGY

Government of Kenya
Ministry of Information Communications and Technology
Telposta Towers, 10th Floor, Kenyatta Ave
Nairobi, Kenya

February 2014

Executive Summary

Global information and communication technology (ICT) growth has transformed how individuals, businesses, and governments produce and receive information. Adoption of ICT into everyday life is widespread in Kenya. The Government of Kenya is proud of this development and is actively encouraging its continued growth through national initiatives such as Kenya's Vision 2030, ICT Master Plan, and the recent deployment of nationwide fiber-optic network infrastructure. Such efforts provide a dramatic increase in interconnectivity among businesses and individuals throughout Kenya. Kenyan public and private sector organizations are now using this increased bandwidth and ICT capabilities to efficiently deliver services, conduct business transactions, and share information across organizational, social, and geographic boundaries.

As Kenya matures into an information society the nation faces an increasingly evolving cyber threat landscape. Nation states, criminal organizations, and hacktivists from all over the world are—and will continue—to exploit ICT vulnerabilities in Kenya. This is simply a reality that every nation with robust ICT infrastructure faces. While these actors seek to illicitly access, alter, disrupt, or destroy sensitive personal, business, and government information, we are working diligently to evolve our means of protecting information in order to counter today's threats as well as those coming from over the horizon.

In response to these threats, and in direct support of the national priorities and ICT goals defined in Vision 2030, Kenya's ICT Ministry developed a National Cybersecurity Strategy (Strategy). The Strategy defines Kenya's cybersecurity vision, key objectives, and ongoing commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructures.

The Government of Kenya is committed to the safety, security, and prosperity of our nation and its partners. We see cybersecurity as a key component in that commitment, providing organizations and individuals with increased confidence in online and mobile transactions, encouraging greater foreign investment, and opening a broader set of trade opportunities within the global marketplace. Successful implementation of the strategy will further enable Kenya to achieve its economic and societal goals through a secure online environment for citizens, industry, and foreign partners to conduct business.

Cybersecurity is a shared responsibility. The Government of Kenya will continue to partner with government, private sector, academia, and other non-government entities to implement our Strategy in the most efficient and effective way possible. We have every confidence that we will meet these challenges together and increase recognition of Kenya as a trusted partner and cybersecurity leader in the East African Community (EAC), Africa, and the world.

INTRODUCTION

The Importance of Cyberspace

Cyberspace is more than just the Internet and information and communications technology (ICT). It is a domain similar to the domains of land, air, sea, and space, but with its own distinct characteristics and challenges. The cyber domain is characterized by the digital storage, modification, and exchange of data via networked systems and supported by critical information infrastructures. It has national and international dimensions that include industry, commerce, intellectual property, security, technology, culture, policy, and diplomacy. As such, cyberspace plays a critical role in the global economy.

Similar to other nations with a robust ICT infrastructure, Kenya's conducts its social, economic and national security activities in this digital, interconnected environment. For example, the Government of Kenya relies on common infrastructure, information technology (IT) platforms, and new technologies to increase the efficiency and effectiveness of government services. One of the main priorities of the Government of Kenya towards the realization of national development goals and objectives for wealth and employment creation, as stipulated in the Kenya Vision 2030, is to achieve an e-Government capability. At the same time, the development, implementation, and adoption of technologies such as mobile computing, mobile banking, and broadband communications enables Kenyans to connect with a speed and ease—unthinkable only five years ago.

However, these same technologies can present new risks that can cause widespread damage to national security, economic growth, and critical infrastructures. Moreover, the reach and impact of cyberspace is accelerating across the national and international boundaries, making it a complex challenge for any government to address alone. For this reason, the Government of Kenya considers securing its national cyberspace a national priority to continue to facilitate economic growth for the country and its citizens.

Government of Kenya Cybersecurity Implementation Hierarchy

ICT growth is particularly prevalent in Africa, where technological advancement and innovation are driving progress in key sectors (e.g., agriculture, education, financial services, government, and health). In 2009, the regional fiber-optic underwater cable increased ICT mobilization and interconnectedness across Kenya and much of East Africa.

With the rapid growth of technology, the Kenyan people have quickly become accustomed to and dependent on the services provided to them through government and business websites, banking connectivity with central banks and other individuals, and ease of communications. These advances continue to bring new and exciting opportunities to businesses and individuals across Kenya.

According to statistics released by The Communications Authority of Kenya (CAK), Kenya had an estimated 16.4 million Internet users and 30.7 million mobile network subscribers as of the second quarter of fiscal year 2012/2013

(source: http://www.cck.go.ke/resc/downloads/Sector_statistics_for_Quarter_2_-_2012-2013.pdf)

THE CYBERSECURITY CHALLENGE

The Evolving Threat Landscape

Aggressively supporting the technological advancements in Kenya has resulted in a more open, interconnected nation which can offer adversaries avenues for exploiting computer networks. Cyber attacks are continuously evolving—to a great extent faster than cyber defences—resulting in an ever-increasing frequency of attacks and the probability of success over time. *Figure 1* provides a snapshot of the sophistication of cyber-attacks from 1980-2012. These cyber attacks may come from hacktivists seeking to publicize political views, from criminal organizations seeking financial gain, from terrorist groups seeking to inflict economic or political damage, or from state-sponsored intelligence and security organizations advancing their own economic or national security aims. Many attacks involve extremely sophisticated technological and social engineering techniques; however, low-technology penetrations—such as insider threats—remain a danger.

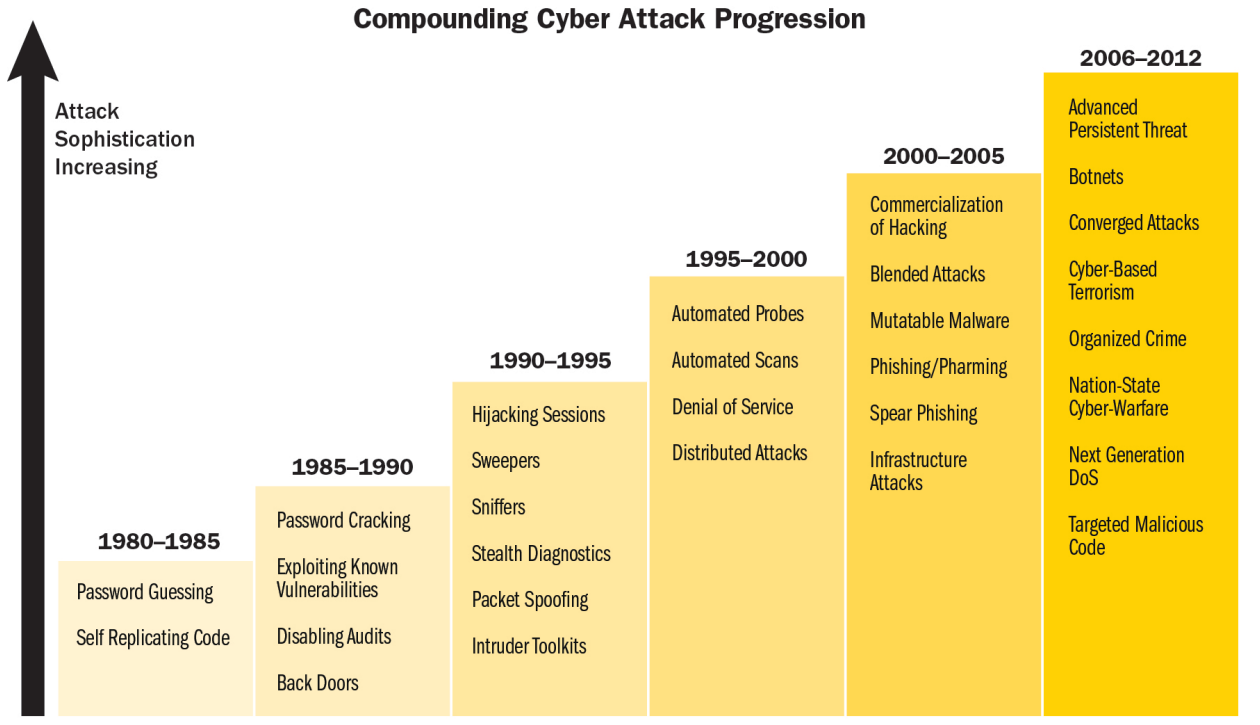


Figure 1: Compounding Cyber Attack Progression

Cybersecurity—a National Priority

The expansive and dynamic nature of ICT creates a wide and deep range of challenges. The Government of Kenya is addressing these challenges to provide for cybersecurity at the national level, enabling economic growth and protecting the interests of the Kenyan people. In evaluating the potential paths forward, the Government of Kenya identified several key challenges resulting directly from emerging risk areas inside Kenya, the East Africa Community (EAC), and internationally. By addressing these risks and understanding the impact of Kenya's cybersecurity efforts, technology growth and economic development will be significantly enabled by cybersecurity implementation.

Both financial and non-financial institutions need high awareness of the need for secure online systems. This will ensure a secure online environment for conducting business and other economic activities. Encourage the use of security standards while designing, building and deploying IT systems.

(source: http://www.ict.go.ke/docs/MasterPlan2017.pdf)

Risks and challenges can manifest from various sources—even from those areas where technology is enabling significant growth and prosperity. For example—by providing people with the ability to access and exchange information, they become dependent on that information to socialized with family and friends, conduct business, and feel connected in our modern world. The National Cyber Security Master Plan addresses emerging cyber risks and the challenges that the ICT may face in the future.

Recognizing this and understanding the critical role ICT plays in Kenya's economy, the Government of Kenya developed the National Cybersecurity Strategy (Strategy). The Strategy supports the three pillars of the Vision 2030 and supports other national initiatives such as the National ICT Master Plan[1] (see *Figure 2*). The purpose of the Strategy is to clearly define Kenya's cybersecurity vision, goals, and objectives to secure the nation's cyberspace, while continuing to promote the use of ICT to enable Kenya's economic growth.

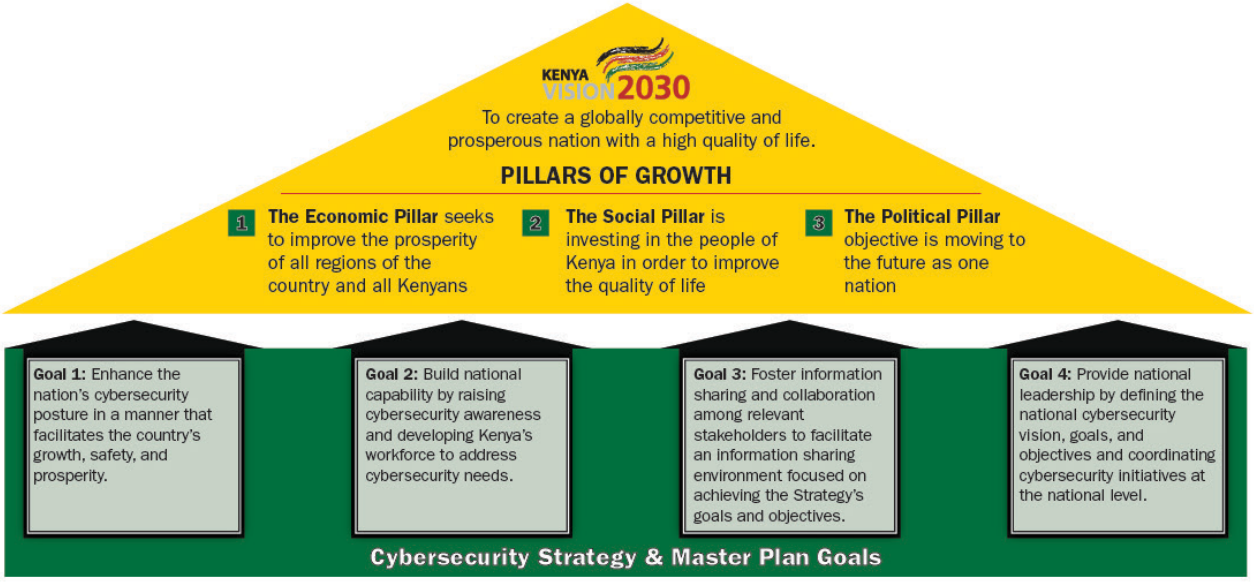


Figure 2: Cybersecurity Strategy Benefits

1 The National ICT Master Plan strategic goals are: (1) every citizen connected; (2) Kenya is Africa's ICT hub; (3) public service for all; and (4) a society built on knowledge.

NATIONAL CYBERSECURITY STRATEGY

To promote the Government's commitment to cybersecurity, the Strategy includes four strategic goals:

1. Enhance the nation's cybersecurity posture in a manner that facilitates the country's growth, safety, and prosperity.
2. Build national capability by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs.
3. Foster information sharing and collaboration among relevant stakeholders to facilitate an information sharing environment focused on achieving the Strategy's goals and objectives.
4. Provide national leadership by defining the national cybersecurity vision, goals, and objectives and coordinating cybersecurity initiatives at the national level.

The subsequent sections outline specific objectives for each goal.

Goal 1: Enhance the Nation's Cybersecurity Posture

Objective: *Protect Critical Information Infrastructure*

The Government of Kenya is promoting ICT usage to both the government and the Kenyan public through an undersea and terrestrial cable and network installations, increased availability of mobile/wireless technology, and a movement towards e-government services. However, the increased use of and reliance on ICT exposes Kenya to increased cyber risks. Threat actors can exploit ICT vulnerabilities to perpetrate crimes against the Government of Kenya and Kenya's citizens who rely on ICT to perform electronic transactions or obtain key critical government services. Also, natural disaster may pose a threat by causing potential damage critical information infrastructure and disrupting communications. As such, it is imperative that as the Government of Kenya protect critical information infrastructure. Its cybersecurity activities should also be flexible enough to counter and mitigate the increasingly complex threats and vulnerabilities to ICT infrastructures.

The Government of Kenya is taking steps to increase the security and resilience of its critical information infrastructure to protect its government, citizens and residents, and corporations from cyber threats and to reap the social and economic benefits of cyberspace. The government is doing this through a coordinated

effort with other countries to increase the security of global cyberspace as a whole. This includes securing critical infrastructures, applications, and services. Additionally, the Government of Kenya is working with relevant stakeholders to build cybersecurity capabilities focused on operations, infrastructure and mission assurance. Within the National Cybersecurity Master Plan the Government has identified a governance and capability structure (Figure 3) which will support scalable growth of cybersecurity within the public and private sectors.

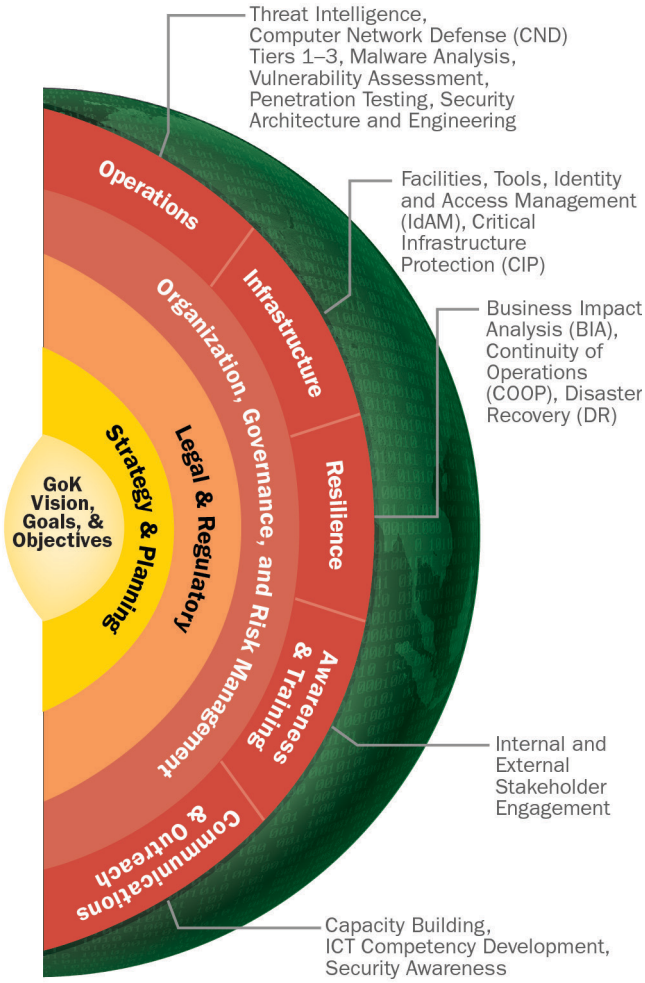


Figure 3: Kenya Cybersecurity Goals and Objectives

Goal 2: Build National Capability

Objective: *Awareness and Training: Inform and educate the Kenyan public and workforce to secure the national cyberspace*

As part of building national capability goal, the Government of Kenya is informing and educating the public and workforce on how to secure the national cyberspace. This includes partnering with other government organizations, the private sector, and academia to ensure that people with cybersecurity responsibilities possess the appropriate level of cyber qualifications and competencies. This effort incorporates human capital management, leadership development, education and training, and strategic communication and change management to develop a nation-wide workforce for the future. Additionally, the Government of Kenya is:

- Working with academia to develop cybersecurity curriculums for higher education and specialized training programs to ensure competency building for cybersecurity professionals; and
- Developing, promoting, and implementing incentive programs to increase the appeal of cybersecurity career paths to attract and retain Kenyans into this critical field.

Objective: *Communications and Outreach: Elevate cybersecurity awareness for government, private sector, and the Kenyan public*

The Government of Kenya is developing, launching, and promoting targeted awareness programs to inform the general public and workforce of common cybersecurity threats and counter measures. Through targeted communications and outreach activities, the Government of Kenya is:

- Increasing the understanding of cyber threats and empower the Kenyan public to be safer and more secure online; and
- Communicating approaches and strategies for the public to keep themselves and their families and communities safer online.

Goal 3: Foster Information Sharing and Collaboration

Objective: *Develop a comprehensive governance framework to leverage resources, reduce conflict and duplication of effort, and work toward Kenya's long-term cybersecurity goals*

Cybersecurity is a complex, multidisciplinary challenge that requires coordination across a wide array of stakeholders. Therefore, implementing the Strategy requires developing a comprehensive governance model that includes meaningful participation by relevant stakeholders, working together toward the common goal of securing Kenya's cyberspace. Through this governance framework, the Government of Kenya intends to:

- Develop the required laws, regulations and policies required to secure the nation's cyberspace;
- Solicits stakeholder input and feedback, as appropriate; and
- Balance information security, privacy considerations and economic priorities.

Cultivate a culture of information sharing that facilitates the real time exchange of cybersecurity information

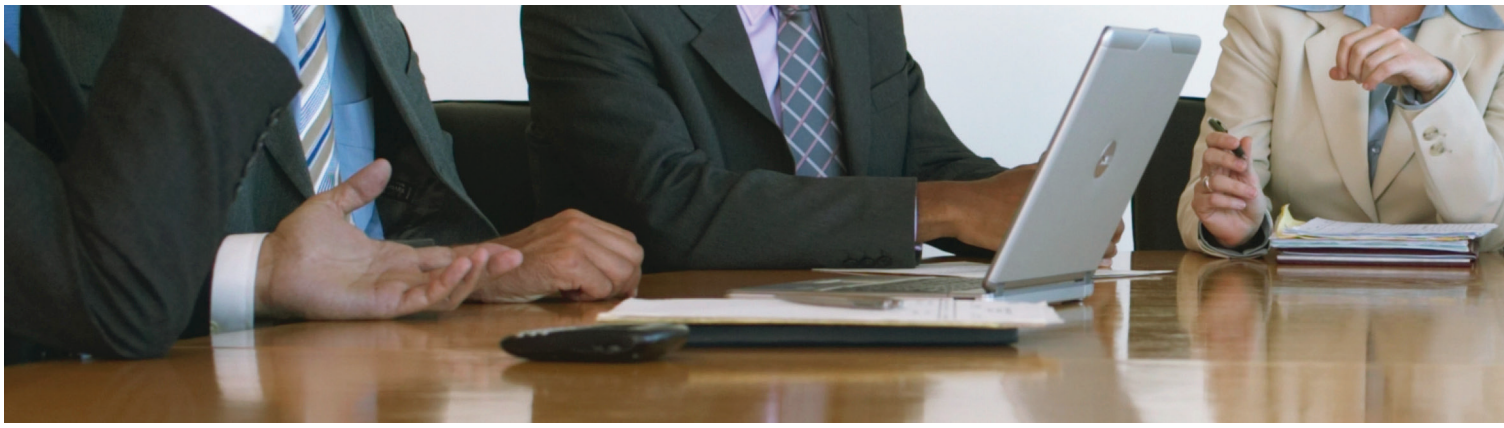
Successful implementation of the Strategy requires the sharing of cybersecurity information (cross-organizational and cross-sector) in a trusted and structured manner. The Government of Kenya will develop and manage a secure information-sharing capability to promote knowledge and lessons learned among relevant stakeholders.

Goal 4: Provide National Leadership

Objective: *Develop and Coordinate Implementation of the National Cybersecurity Strategy and Master Plan*

Enhancing Kenya's cybersecurity posture is a top priority for the Government of Kenya. As such, the Government of Kenya will continue to provide a single, unified agenda that will guide all relevant national stakeholders. Specifically, the ICT Ministry will:

- Continue to refresh the Strategy (vision, goals, and objectives), as required and establish a tactical roadmap for achieving national cybersecurity objectives; and
- Use the Strategy, and complementary Cyber Security Master Plan to identify and implement relevant cybersecurity initiatives, in conjunction and in collaboration with relevant stakeholders.



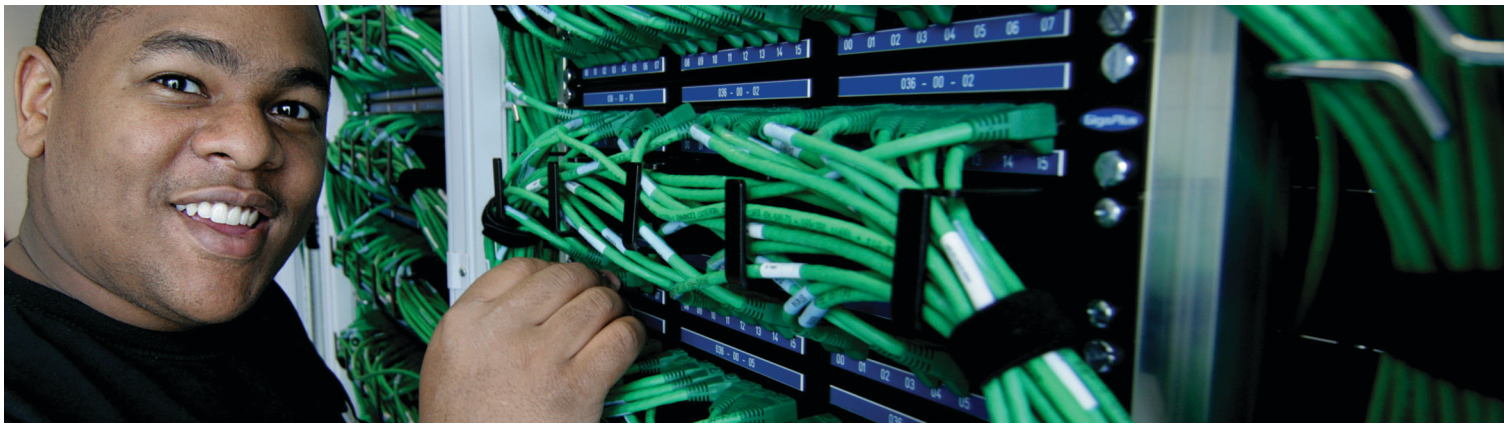
KEY BENEFITS

The Government of Kenya expects to see considerable benefit from the development of a holistic national cybersecurity strategy. These benefits will be realized, not only within ICT circles, but across social and economic areas by all Kenyans.

These benefits clearly impact and improve the Pillars of Growth established by Kenya Vision 2030: The Economic Pillar, The Social Pillar, and The Political Pillar by directly supporting the goals of increasing prosperity, improving the quality of life, and moving to the future as one nation.

Benefit Area	Details of Benefits Resulting from Improved Cybersecurity
Private Sector Growth	■ Added e-commerce applications due to a more secure environment ■ Growth in the quantity of e-commerce transactions ■ Lower business risk and uncertainty ■ More competition among firms as secure e-commerce grows ■ Financial sector growth as the number of financial transactions grow ■ More sustainable economic growth through sustained security and increased confidence in e-commerce ■ Through e-markets, suppliers are able to interact and transact directly with buyers, thereby eliminating the costs related to intermediaries and distributors. Businesses can increase revenues and margins
Greater Cooperation with Relevant International Organizations	■ Increased incentives to participate in the formation of international rules, including intellectual property rights, contract law, electronic signatures and authentication, consumer protection, jurisdiction and others; secure electronic commerce issues are addressed in international for a such as WIPO (World Intellectual Property Organization), UNCITRAL (United Nations Commission on International Trade Law), the Hague Conference on Private International Laws, ISO (International Standard Organization) including COPOLCO (Consumer Policy Committee), OECD and others

Benefit Area	Details of Benefits Resulting from Improved Cybersecurity
Improved Organizational Performance and Reduced Transactions Cost	■ Lower costs due to improved efficiency of transactions ■ Lower cost leads to an increase in the number of firms in the market ■ Provides avenues for firms to enter into the business-to-business and business-to-government global supply chains ■ Easier marketing of agricultural products and local sourced goods in the global market ■ Reduction of search costs as buyers and sellers are together in a single online trading community ■ Reduction in the costs of processing transactions (e.g., invoices, purchase orders and payment schemes), with the automation of transaction processes ■ Efficiency in trading processes and transactions as sales can be processed through online auctions ■ Online processing improves inventory management and logistics
Promote Anti-Corruption in Government and Industry	■ Increase in price transparency as the gathering of a large number of buyers and sellers in a single e-market reveals market price information and transaction processing to participants; the publication of information on a single purchase or transaction makes the information readily accessible and available to all members of the e-market ■ Increased price transparency can exert downward pressure on price differentials in the market; buyers are provided much more time to compare prices and make better buying decisions ■ Expansion of borders for dynamic and negotiated pricing wherein multiple buyers and sellers collectively participate in price-setting and two-way auctions; prices can be set through automatic matching of bids and offers; the requirements of both buyers and sellers can be more easily aggregated to reach equilibrium price levels, which are lower than those resulting from individual actions
A More Competitive Business Environment	■ Trade liberalization as cross-border transactions costs decline ■ Resolution of patent issues: international programs will contribute to achieving harmonized patent protection for progress and developments in secure transactions ■ Enhanced public welfare through improved access to online goods and services ■ Greater social cohesion as wage and income disparities lessen due to improved communication and information sharing, i.e., a better functioning labor market ■ More options for consumer transactions (more, reliable distribution channels) ■ Lower transactions costs ■ Lower prices in longer term
Transparency and Efficiency in Government	■ Expedited government financial transactions enabling greater efficiency and expediency in resource allocation ■ Improved communications



CONCLUSION

As Kenya's remarkable ICT growth continues, ensuring the confidentiality, integrity, and availability of public and private sector information across Kenya's ICT infrastructure is of significant importance. Kenya's National Cybersecurity Strategy serves to demonstrate the government's commitment to improving Kenya's cybersecurity posture and share overarching vision, goals, and objectives. Implementation of the strategy is supported by an evolving national Cybersecurity Master Plan, which has been developed to define (and ultimately govern) a prioritized roadmap of discreet cybersecurity projects.

Both the strategy and master plan are critical to securing the online environment for citizens, industry, and foreign partners; increasing the Kenyan people's confidence in online transactions, data security, fraud protection, and privacy; encouraging greater foreign investment and enhancing trade opportunities; and enabling Kenya's broader economic and societal goals.

TERMS AND DEFINITIONS

Term	Definition
Broadband	A type of high-capacity telecommunications especially as used for access to the Internet.
Computer Incident Response Team	The personnel responsible for coordinating the response to computer security incidents within an organization
Critical Infrastructure	A term used to describe assets that are essential for the functioning of a society and economy. (e.g., electrical grid, telecommunications, water supply)
Cybersecurity	The processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction
Cyberspace	The notional environment in which communication over computer networks occurs
e-Government	Short for electronic government, it is digital interactions between a government and citizens, government and businesses, government and employees, and also between two governments
Globalization	Growth to a global or world-wide scale
Governance	Consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility
Information and Communication Technology (ICT)	The applications of computers and telecommunications equipment to store, retrieve, transmit and manipulate data

Term	Definition
Insider Threat	A malicious individual who is also an employee or officer of a business, institution, or government
Social Engineering	A non-technical kind of intrusion (or "hack") that relies heavily on human interaction and often involves tricking other people to break normal security procedures

GOVERNMENT of KENYA
CYBERSECURITY STRATEGY