BIZCOMMUNITY

# What's been done to fight cybercrime in East Africa

By Mercy Muendo

3 Dec 2019

East Africa attracts millions of tourists every year. Over the past 10 years, its earnings from tourism have doubled. Compared to the rest of Africa, the region is experiencing healthy economic growth. This makes it a promising investment destination.

Cyber insecurity is a threat to Africa's digital economy. Riccardo Mayer/Shutterstock

Factors like regional tourism, movement of workers and technology development have catalysed East African integration and cross-border banking.

Many cross-border banks originate from Kenya with branches across the region. One example is Kenya's Equity Bank, which relies heavily on digital technology. The digital space has many positive attributes but the threat of cybercrime and insecurity is prevalent.

Uganda lost 42 million shillings to cybercrime in 2017. In 2018, Rwanda lost 6 billion francs. In Kenya, between April and June 2019 alone, the country experienced 26.6 million cyber threats.

Across the region, with the increase of digital banking, financial institutions have become targets. These institutions are attractive to cyber criminals because they hold the biggest cash reserves. Africa's digital infrastructure is ill-equipped to manage the continent's growing cyber-security risk.

Equity is a pioneer in online and mobile banking with technology that merges banking and telephony. However, it recently suffered a cyber-attack. Last month, Rwandan authorities arrested a cybercrime syndicate comprising eight Kenyans, three Rwandans and a Ugandan. The syndicate had attempted to hack into the Equity Bank system. The group has been involved in similar attacks in Kenya and Uganda.

Early in the year, Kenya's director of criminal investigation issued warrants of arrest against 130 suspected hackers and fraudsters for alleged banking fraud.

These incidents show that financial losses to cyber insecurity are a growing threat to East Africa's economy.

Cybercrime occurs through the use of computers, computer technology or the internet. It often results in identity theft, theft of money, sale of contraband, cyber stalking or disruption of operations.

Within East Africa, Kenya, Rwanda and Uganda are taking steps to manage the huge cybercrime risk. But the cyber attack on Equity Bank is proof that these countries need to do more to protect their financial institutions from massive losses going forward.

## Regional instruments

The African Union’s Convention on Cyber Security and Personal Data Protection is East Africa’s overarching policy guideline on cybercrime. It was adopted by member states in 2014. The policy is similar to the Council of Europe’s Cyber Crime Convention which established a cyber security on the European continent.

Rwanda signed the convention earlier this year, but it’s the only East African country to have done so.

The convention requires member states to share responsibility by instituting cyber security measures that consider the correlation between data protection and cybercrime. These measures will keep data safe from cyber criminals and preempt its misuse by third parties. It also encourages the establishment of national computer emergency response teams.

In addition it advocates closer cooperation between government and business, and creates a provision for dual criminality. This means that cybercrime suspects can be tried either in the country where the crime was committed or in their home country. This provision is meant to ensure smooth cooperation and sidestep any conflict of laws.

There is also a provision on mutual legal assistance. This allows for member states to share intelligence and collaborate on investigations.

Even though Uganda and Kenya aren’t yet signatories, they have nevertheless been establishing legal and policy frameworks provided for under the convention. Rwanda is doing so too, and as a signatory is one step ahead.

## Rwandan approach

In 2015, Rwanda came up with a national cyber security policy that established a National Computer Security and Response Centre. The centre detects, prevents and responds to cyber security threats. And in 2016, the Regulatory Board of Rwanda Utilities rolled out network security regulations to protect the privacy of subscribers. They also empower the government to regulate and monitor internet operators and service providers.

The country also has a National Cyber Contingency Plan to handle cyber crises.

Further, Rwanda’s telecom network security regulations require service providers to secure their services by protecting their infrastructure. Every service provider must be licensed and must guarantee the confidentiality and integrity of their services. They must also set up incident management teams. These teams work with the government to manage cyber security threats effectively.

Additionally, Rwanda passed an information and communication technology law in 2016. This contains provisions on computer misuse and cybercrime which criminalise unauthorised access to data.

The country has managed to build the foundations of a strong regulatory framework. It has also taken measures to raise awareness around cyber security. In fact, in the attack on Equity Bank, the authorities acted on a tip from members of the public.

## Kenyan measures

In 2014, Kenya launched its National Cyber Security Strategy to raise cyber security awareness and equip Kenya's workforce to address cyber security needs.

In line with this strategy, Kenya amended its information and communications law to criminalise unauthorised access to computer data.

Kenya has also set up a national computer incident response coordination centre to consolidate key cyber infrastructure and create pathways for regional and international partnership.

Generally, Kenya has a robust cyber security policy which includes a legal and regulatory framework. The result has been that impending cyber attacks are discovered before massive damage is done and ongoing attacks are rapidly arrested.

## Uganda's security

Uganda has legislation to protect cyber security. This includes the Computer Misuse Act which ensures the safety and security of electronic transactions and information systems, and the Regulation of Interception of Communications Act to monitor suspicious communications. It also has a national computer emergency response team.

This regulatory framework is similar to those in Kenya and Rwanda. But in addition, Uganda has a National Information and Technology Authority that provides technical support and cyber security training. It also regulates standards and utilisation of information technology in both the public and private sectors. These measures have boosted the countries' cyber security strategy.

While Uganda has these measures in place, Kenya and Rwanda are two of the top three cyber secure countries in Africa.

## Moving ahead

Kenya, Uganda, and Rwanda have taken solid steps to harmonise cybersecurity processes, data protection, and collaborative prosecution and investigation measures.

They have criminalised cybercrime and established frameworks to manage cyber attacks. International cooperation within the region has also enhanced cyber security.

ABOUT THE AUTHOR

Mercy Muendo, lecturer, information technology and the law , *Daystar University*