Kenya's Experience in Cyber-Security Management

Increasingly, the world is becoming more connected, thanks to the Internet, a myriad of services that are digitally enabled, low-cost smart devices and emerging online applications. As the use of and dependency on ICTs grow, the risks also increase, including cyber threats and cybercrimes.

The complexities and global nature of the internet call for action on all stakeholders to pull efforts to secure the cyber space. Not only must stakeholders be aware, but they must also arm themselves with the relevant capabilities that help prevent or address the ever-increasing threats and vulnerabilities online.

Kenya is ranked second in Africa, and 44th globally in terms of the Global Cyber-security Index (GCI). In order to enhance the security of the cyber space in Kenya, and in line with the Kenya Information and Communication Act (KICA) and the National Cyber-security Strategy, Kenya's ICT sector regulator - the Communications Authority of Kenya (CA) - has set up the National Kenya Computer Incident Response Team - Coordination Centre (KE-CIRT/CC) to handle coordination and response to cyber threats as well as act as Kenya's national point of contact for cyber security matters.

The National KE-CIRT/CC, established with support of partners such as the International Telecommunication Union (ITU) through the Global Cyber-security Agenda; works together with various stakeholders at both local and international levels to execute its mandate.

With increasing cyber-attacks such as online fraud, malware attacks, identity theft and impersonation, KE-CIRT/CC continues to play a critical role such as thorough monitoring and issuing cyber threat advisories. For instance, during the October - December 2019 period, the National KE-CIRT/CC detected 37.1 million cyber threats as compared to 25.2 million cyber threat events detected in the previous quarter, representing a 47.3 percent increase. In the same period, they issued 16,637 cyber threat advisories

Successfully also, the Authority has been able to institute a Child Online Protection (COP) initiative that aims to protect and encourage the youth to be responsible digital citizens and to build the capacity of cyber-security professionals (CISOs) to deal with the cyberspace within their workplaces. Other areas of collaboration include technical assistance in response to cyber threats, investigations and prosecutions as well as through enhancement of Mutual Legal Assistance Treaty (MALT) between international actors.

In May 2019, the European Union passed the General Data Protection Regulations commonly known as GDPR, which inspired the enactment of the Data Protection Act and the Computer Misuse and Cyber Crimes Act, by Kenya, to ensure consumer data is safeguarded against misuse.

Despite these levels of success, the sector has been dogged with many challenges such as: lack of uniform community standards across various jurisdictions on internet use by service providers, shortage of technical and professional capacity and lack of a uniform certification policy for cyber-security professionals.

Going forward, a lot more needs to be done with the goal of making cyberspaces more secure and resilient for use. Collaborations and partnerships will make this path more realistic.