A Collaborative Approach to National Cybersecurity Resilience

ISACA Conference 2019
Communications Authority of Kenya

Section 83C of KICA (1998) mandates the CA to:

- Promote and facilitate the efficient management of critical Internet Resources;
- Develop a framework for facilitating the investigation and prosecution of cybercrime offences;
- Facilitate electronic commerce and eliminate barriers to electronic commerce; and
- Develop regulations with respect to Cybersecurity, E-Transactions, Electronic Certification and Domain Name Administration.
Cybersecurity Instruments

- VISION 2030
- ICT Sector Policy
- National Cybersecurity Strategy
- KICA (1998)
- National KE-CIRT/CC
- NPKI
Kenya’s Cybersecurity Governance Structure

- National Security Council (NSC) (Chaired by the President)
- National Security Advisory Committee (NSAC) (Chaired by the Head of Public Service & Chief of Staff)
- National Cybersecurity Steering Committee (NCSC) (Chaired by the PS/MoICT)
- National KE-CIRT/CC (Coordinated by CA)
- Threat Intelligence (Coordinated by NIS)
- E-Government Programmes (Coordinated by ICTA)
The National KE-CIRT/CC

Mandate
To offer advice on Cybersecurity matters nationally; and to coordinate response to cyber incidents in collaboration with relevant stakeholders.

Role
Kenya’s national point of contact on cyber security.
Functions of the National KE-CIRT/CC

- Implement National Cybersecurity Policies, Laws & Regulations
- Cybersecurity Awareness & Capacity Building at the National Level
- Technical Co-ordination & Response to Cybersecurity Incidents
- Early Warning & Technical Advisories
- Development & Implementation of a National Public Key Infrastructure (NPKI)
- Research & Development (R&D) on Cybersecurity
- Establish Collaboration (National, Regional & International) on Cybersecurity
What Does Collaboration Entail?

Ideally, it means…

Public and Private sectors working together to enhance our national cybersecurity readiness and resilience through sharing insights, intelligence, expertise, facilities and personnel.
Why Collaboration?

- Cyber threats are evolving and no one organization or sector can mitigate the risks posed by cyber threats.
- Cyber threats are a societal problem that affect us all, with all sectors significantly affected by cyber security.
- Protecting our critical national infrastructure requires a collaborative approach to ensure that organizations are able to manage cyber risks in a way that is cross-industry in perspective.
The Conversation on Collaboration...

- Interplay between roles, responsibilities and obligations of the various sectors and players.
- Contradictory obligations – social, economic, national security.
- Trade off between cybersecurity and other values.
- Societal and personal nature of cyber security.
What are the Key Challenges of collaboration?

- Lack of trust
- Leadership challenges?
- Privacy concerns
- Protection of intellectual property
- Assignment of roles and responsibilities
- Too many parties involved
- Lack of standards or guidelines
- Selecting the rights partners to collaborate with
What are Some of the Reference Points for Collaboration?

- Research & development
- Information sharing
- Assigning of roles
- Notification requirements
- Duty of assistance
- Active defense
Collaboration Outcomes

- Research and development
- Interagency collaboration
- Information sharing
- Alignment of standards, capacities and outcomes across the cyber security value chain (demolishing the silos)
What Must We Do?

- Advancing cyber resilience requires collaboration in new and innovative ways.
- Need to have discussions on building institutions, frameworks, polices, norms and processes necessary to support collaboration.
- Need to be inclusive in representing and negotiating between interests and principles.
Government’s Role

- Put in place an effective collaboration model, clear goals, guidelines, standards, frameworks, infrastructure, and personnel to effect collaboration.
- Develop a foundation for the coordinated, informed and effective coordination and response to cyber crime.
- Establish an environment that guides all stakeholders towards shared goals, while retaining overall accountability, oversight, governance and ownership of major initiatives and outcomes.
- Facilitate purposeful, effective, and meaningful collaboration between all stakeholders so as to achieve aligned outcomes and a ‘no man left behind’ approach.
- This has been set out by the creation of the National KE-CIRT/CC
Local Collaborative Efforts of the National KE-CIRT/CC

- On the national level the National KE-CIRT/CC collaborates with various stakeholders through the National KE-CIRT/CC Cybersecurity Committee (NKCC).

- Some of the committee members are:
  - Law enforcement agencies,
  - ICT Authority (ICTA)
  - Internet service providers (ISP)
  - Telecommunication operators
  - Academia
  - The banking/financial sector, among others.
Local Collaborative Efforts of the National KE-CIRT/CC

- Law Enforcement Agencies
- Government agencies
- Banking and Financial Services
- Directorate of Public Prosecutions (DPP)
- Mobile Telecom Operators & ISPs
- Academia
- Banking and Financial Services
Global Collaborative Efforts of the National KE-CIRT/CC

Northern Corridor Integration Projects - NCIP
Input Needed for Collaboration

“Active participation and a willingness to contribute in a meaningful way to the National Cybersecurity Strategy and combine efforts towards achieving mutually beneficial outcomes.”