KICTAnet
KENYA ICT ACTION NETWORK

The Secretariat,
Director Programmes & Standards, ICT Authority
Telposta Towers, 12th Floor, Kenyatta Avenue,
P. O Box 27150-00100 Nairobi.
To: critical@ict.go.ke,pnyambura@ict.go.ke.

21 April 2015

Kenya ICT Action Network (KICTANet)'s input into the proposed Critical Infrastructure Bill

Acknowledge

ICT is a tool that is critical for operations and hence requires specialized attention: availability, integrity, and confidentiality.

Starting point:

1. Have criteria for defining what critical ICT infrastructure is.
2. Distinguish between critical ICT infrastructure (Registry, content delivery networks) and traditional critical infrastructure.
3. Question if there is need to put transport and energy infrastructure on the Internet and if so, how is it protected? Anything put on the internet is vulnerable.
4. Acknowledge that business models of ICT companies are different from the traditional models of non-ICT critical infrastructures such as energy utilities and industrial control systems. They require more maintenance and upgrades that translate into much more investments.
5. How do we ensure we have scalable and resilient critical infrastructure? In the past we have seen government institutions invest in white elephants, sending them back to the procurement room before the system goes live.
6. Consider the need for expertise to deal with and protect the infrastructure (developers focusing on software security and information security professionals specializing in critical infrastructure).
7. Consider cybersecurity but avoid raising fear, uncertainty and doubt.

8. Avoid any type of strategy that hacks back. Hacking back will not fix broken infrastructure, and the attribution problem makes it very hard and sometimes impossible to find the real source of attacks. Focus on defense and resilience.
9. Need to have websites running latest versions of software including security updates otherwise we will continue to experience this: https://www.google.com/#q=%22hacked+by%22+site:go.ke. There should be a big focus on identifying XP use and migrating away from XP usage in government and critical infrastructures.

Management questions

10. Who manages critical infrastructures?
11. Should the government own/manage/handle infrastructures like the NOFBi?
12. Which infrastructure can the government outsource? Which infrastructure is a security threat to outsource? Who are trusted partners for outsourcing?
13. What is the value of investment in NOFBI while there is no last-mile connectivity? Should the NOFBI operator be able to go the long haul and provide last-mile services to all intended recipient(s) of the service?
14. What levels of approvals are there (change management) for any change to happen in a critical internet resource? (Just last month, a misguided change at KENIC affecting DNSSEC affected the entire .ke domains for a whole day. No domain was accessible).
15. How is the security and integrity of PKI maintained?
16. How are the counties managing ICT county-specific infrastructure and what capacities exist at that level?

Roll out/ Rapid Response questions

17. How fast can we roll out, upgrade, and repaired our fiber optic infrastructure? (There has been a deliberate systematic plot to ensure there are no ducts on wayleaves to pull fiber optic cable within minimum time, and cost-effectively).
18. Can we vet the software that runs on and support critical infrastructure? We have had cases of defective and compromised firmware and compromised software that has payloads executed at certain times by malicious actors. Which software and hardware do we trust? Can we audit this software?

19. What is the role of standards? (ISO 27000 series Standards on Information Security and the ISO 20,000 series on Service Management).

Regulation vs Legislation and questions regarding scope

20. Is it necessary to have an Act on critical infrastructure considering the dynamism and complexity of ICT? Would a few amendments under the KICA 2013 not suffice?
21. Would it perhaps not be useful to have separate acts or regulations for critical internet infrastructure on the one hand, and critical infrastructures like (power and transport) connected to the internet on the other hand? The two types of critical infrastructure are related but require different and specialized approaches.
22. The development of a critical infrastructure policy framework should precede the bill to contextualize the Critical Infrastructure bill. The policy framework should also have an implementation framework, a result of which could be the development of law. Before the development of the policy it may be necessary to conduct a study and expert consultation on the matter that includes a review of global best practices.
23. The protection of critical infrastructure may be better managed under regulations rather than Bills/Acts. This is because in the fast-changing world of IT, what is critical today may not be tomorrow and vice versa. Who would have known five years ago that M-PESA would move beyond just sending money, to becoming a lifestyle for millions of Kenyans aka a critical infrastructure? You don’t manage such issues through hard-wired Acts, but through Regulation.

Recommendations on Policy and law

The said policy and law should clearly outline:

- Definition of what constitutes critical infrastructure.
- Distinguish between critical internet/ICT infrastructures and critical infrastructures connected to the internet.
- Criteria for identification of CI.
- Threat analysis to various CI in Kenya.
- A risk management framework for the CI.
- The requirement of mandatory minimum protection of critical infrastructure as well as demonstrated assurance through compliance.

- Coordination framework (including PPP arrangements, lead coordinating org, and perhaps the need for a single body?).
- Investigate frameworks for threat intelligence and information sharing between all concerned stakeholders.
- Incident reporting mechanisms and investigations of possible requirements for breach disclosure to all affected stakeholders.
- Research and development strategies.
- Capacity assessment and development.
- Funding mechanisms.
- Implementation plan.

Note: It will be important for institutions (private and public) to meet the law and associated regulatory requirements (Consistent with the 2010 constitution). In addition, Institutions must integrate their plans with agencies/bodies (e.g. fire, security, emergency, hospitals, etc.) that are critical to an effective response.

Submitted on behalf of KICTANet by Grace Githaiga, Victor Kapiyo, Barrack Otieno, Mwendwa Kivuva, John Walubengo, Matunda Nyanchama, Alex Comninos and Ali Hussein.